

# Strong authentication for Cisco ASA 5500 Clientless SSL VPN and Cisco VPN Client Solutions with



nordic edge

## One Time Password Server



The complete installation guide for securing the authentication to your Cisco ASA 5500 solution with Nordic Edge One Time Password Server, delivering two-factor authentication via SMS to your mobile phone. For both clientless SSL VPN and Cisco VPN Client.



Content

<b>1</b>	<b>SUMMARY .....</b>	<b>4</b>
<b>2</b>	<b>PREREQUISITES .....</b>	<b>4</b>
<b>3</b>	<b>IMPORTANT INFORMATION REGARDING COMMUNICATION .....</b>	<b>4</b>
<b>4</b>	<b>GETTING STARTED.....</b>	<b>5</b>
4.1	1.1 Download the software .....	5
4.2	Register and download the software.....	6
<b>5</b>	<b>INSTALLATION .....</b>	<b>9</b>
5.1	Start the installation .....	9
5.2	Installing license.....	11
<b>6</b>	<b>CONFIGURING THE ONE TIME PASSWORD SERVER .....</b>	<b>15</b>
6.1	Start the OTP Configuration .....	15
6.2	Server page .....	16
6.3	Plugin manager page .....	17
6.3.1	Nordic Edge SMS Plugin .....	18
6.4	Nordic Edge SMS Page .....	19
6.5	Radius & Client page.....	20
6.5.1	Enable Radius .....	21
6.6	Add client .....	22
6.7	Configure LDAP.....	23
6.7.1	Test LDAP Connection .....	23
6.7.2	Selecting Search Base DN .....	25
6.7.3	Select Search filter .....	27
6.7.4	Test LDAP Authentication .....	29
<b>7</b>	<b>START THE ONE TIME PASSWORD SERVER.....</b>	<b>31</b>
<b>8</b>	<b>ADD MOBILE PHONE NUMBER WITH MICROSOFT MANAGEMENT CONSOLE.....</b>	<b>32</b>
<b>9</b>	<b>CONFIGURING ASA5500 FOR SSL VPN AUTHENTICATION WITH NORDIC EDGE ONE TIME PASSWORD SERVER.....</b>	<b>33</b>
9.1	Start ASA device manager.....	33



<b>9.2</b>	<b>Browse to Configuration, Remote Access VPN, AAA/Local Users, AAA Server Groups and click Add. ....</b>	<b>33</b>
<b>9.3</b>	<b>Name Server Group OTPserver, choose protocol RADIUS .....</b>	<b>34</b>
<b>9.4</b>	<b>Add new radius server to the RADIUS group .....</b>	<b>35</b>
<b>9.5</b>	<b>Configure Radius Server : Interface name, IP address to OTPserver and the pre-shared key between the One Time Password server and Cisco ASA5500. ....</b>	<b>35</b>
<b>9.6</b>	<b>Create a "test" connection profile (in case you want to test this for certain users only). 37</b>	
9.6.1	Browse to Configuration/Remote Access/Clientless SSL VPN Access/Connection Profiles and click Add .....	37
9.6.2	Specify Connection Profile Name .....	38
9.6.3	Specify AAA Server Group = OTPserver .....	38
9.6.4	Edit Connection Profile Clientless SSL VPN Settings .....	40
9.6.5	Add Alias if user should be able to select authentication method by drop-down-list .....	40
9.6.6	Edit Connection Profile Clientless SSL VPN Settings .....	41
9.6.7	Add Group URL if user should be able to select authentication by specifying URL .....	41
9.6.8	If user should be allowed to select authentication method by drop-down-list, .....	41
9.6.9	select this item. ....	41
<b>10</b>	<b>CONFIGURING ASA5500 FOR CISCO VPN CLIENT AUTHENTICATION WITH NORDIC EDGE OTP SERVER .....</b>	<b>45</b>
<b>10.1</b>	<b>Add a new ( or Edit an existing) Cisco VPN Client Connection Profile to use the OTPserver.....</b>	<b>45</b>
<b>10.2</b>	<b>At the Cisco VPN Client, create an entry with correct name and password .....</b>	<b>46</b>
<input type="checkbox"/>	<b>Name must match the connection profile name at previous slide.....</b>	<b>46</b>
<input type="checkbox"/>	<b>Password must match the pre-shared key in ASA5500. ....</b>	<b>46</b>
	<b>(Note : This can be distributed via MSI installation).....</b>	<b>46</b>
<b>11</b>	<b>START TESTING .....</b>	<b>47</b>
<b>11.1</b>	<b>Enter your Userid and password as usual.....</b>	<b>47</b>
<b>11.2</b>	<b>You will receive a one-time password to your mobile phone within a couple of seconds. 47</b>	
<b>11.3</b>	<b>Enter your one time password and click on "OK" .....</b>	<b>48</b>
<b>12</b>	<b>PURCHASE.....</b>	<b>49</b>
<b>13</b>	<b>TECHNICAL QUESTIONS.....</b>	<b>49</b>



## 1 Summary

This is the complete installation guide for securing the authentication to your Cisco ASA 5500 solution with Nordic Edge One Time Password Server, delivering two-factor authentication via SMS to your mobile phone. For both clientless SSL VPN and Cisco VPN Client. You will be able to test the product with your existing Cisco ASA 500 and LDAP user database, without making any changes that affect existing users. The guide will also allow you to make the complete installation efficiently, using a maximum of 1 hour. Nordic Edge provides several methods for delivering one time passwords, like e-mail, tokens, mobile clients, prefetch etc. - however in this test we are only going to use SMS.

This is a step-by-step guide that covers the entire installation from A to Z. It is based on the scenario that you are running your Cisco 5500 solution against Active Directory, and that you install the One Time Password Server on a Windows Server. The One Time Password Server is platform independent and works with all other LDAP user databases, like eDirectory, Sun One, Open LDAP etc. If you are not running Active Directory or Windows and if you have any questions regarding the slight differences in the installation process, you are most welcome to contact us at [support@nordicedge.se](mailto:support@nordicedge.se) and we will take you through the entire process.

## 2 Prerequisites

You will need to have a server available, for example a VMware virtual machine with Windows Server 2003 installed with Ethernet in bridge mode. The server needs to have an ip-address configured and must also be able to reach your DNS-servers, your Cisco 5500 ASA solution and the Active Directory. Since the software is quite small and easy to remove, you can also use any existing server in your network.

## 3 Important information regarding communication

The One Time Password Server is a software that you can place on any server in your internal network or DMZ.

- The One Time Password Server needs to be able to communicate (Outbound traffic) with your **LDAP** or **JDBC** User Database. Default port for LDAP and Secure LDAP is TCP port 389 / 636.
- The Integration Module needs to be able to communicate (Outbound traffic) with the One Time Password Server on TCP port 3100. Or Radius with UDP port 1812 or 1645 (Outbound traffic)
- If you want to use the **Nordic Edge SMS Gateway**, the One Time Password Server needs to be able to communicate (Outbound traffic) with [otp.nordicedge.net](http://otp.nordicedge.net) and [otp.nordicedge.se](http://otp.nordicedge.se) with HTTPS on TCP port 443.

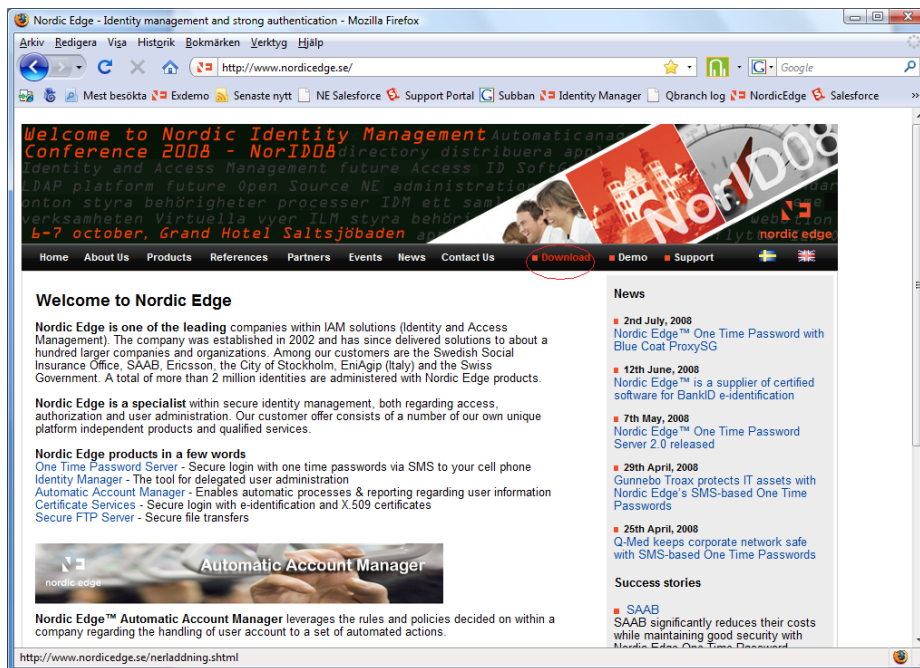
In this test-scenario you will want to communicate with RADIUS port 1812 or 1645 and use our Nordic Edge SMS Gateway.



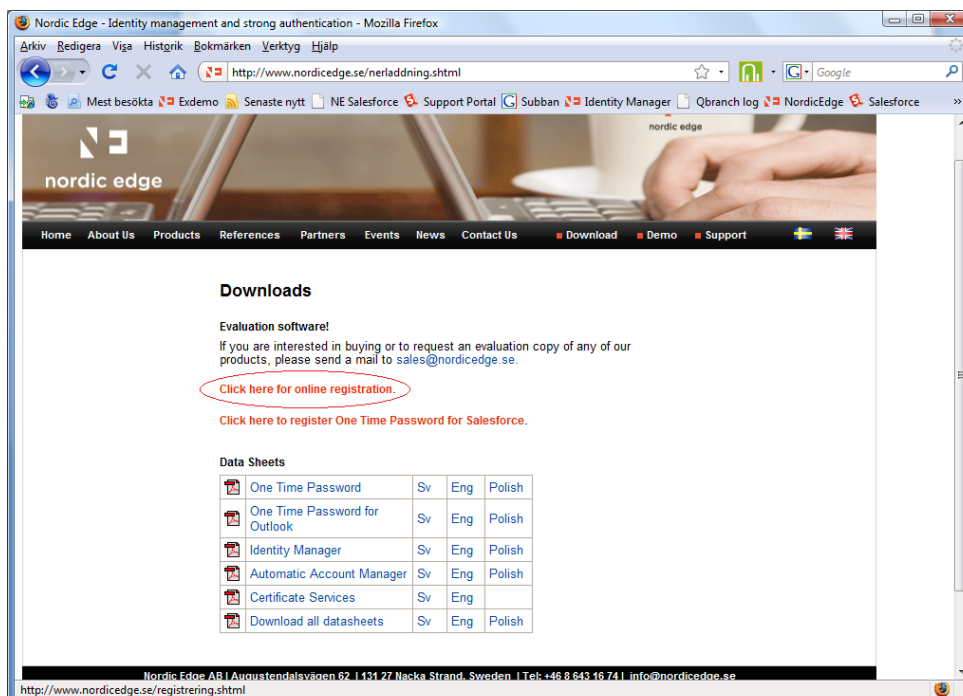
## 4 Getting started

### 4.1 1.1 Download the software

Go to [www.nordicedge.se](http://www.nordicedge.se) and click on Download



## 4.2 Register and download the software

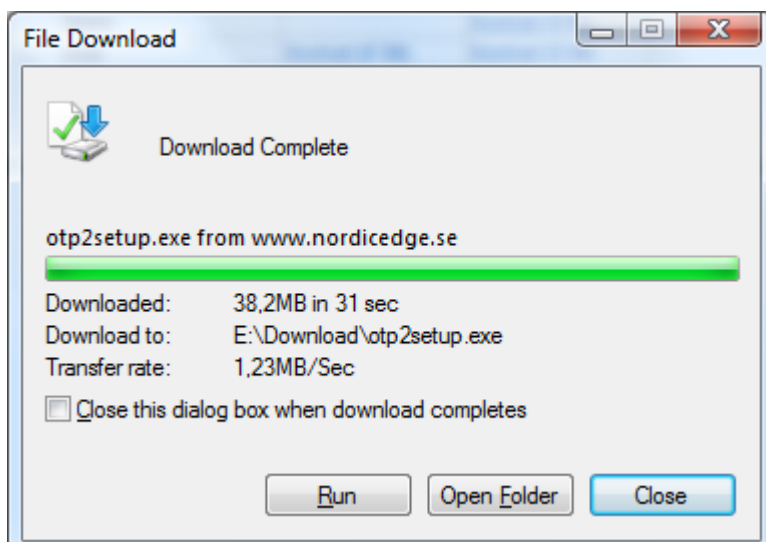
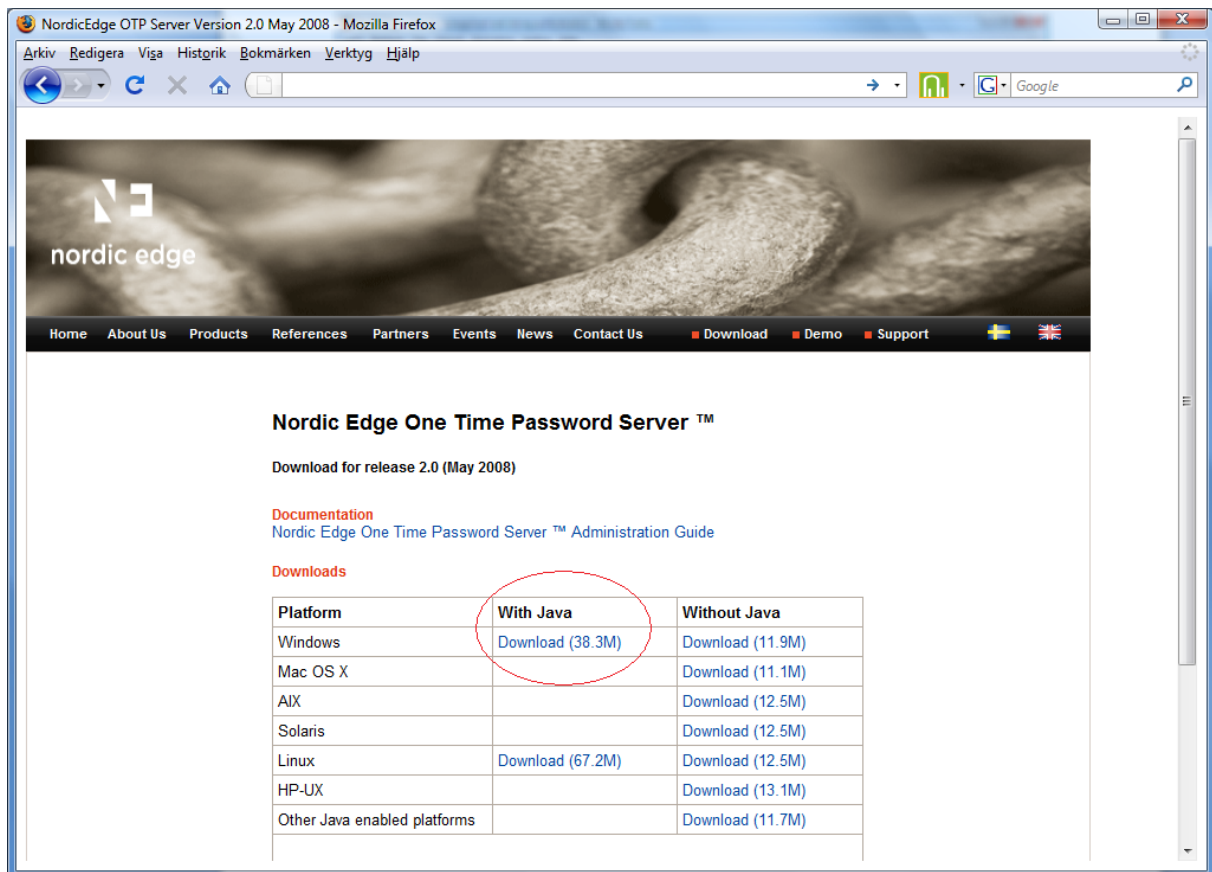




The screenshot shows a web browser window titled "Nordic Edge - Identity management and strong authentication - Mozilla Firefox". The address bar shows the URL "http://www.nordicedge.se/registrering.shtml". The page features the Nordic Edge logo and a navigation menu with links: Home, About Us, Products, References, Partners, Events, News, Contact Us, Download, Demo, and Support. The main content area is titled "Software Evaluation Registration Form" and includes a brief description: "Please fill in this form to get an evaluation of our software. On submit, a mail will be sent to the registered address, with information on how to download the software. Upon download of the software, a 30 day evaluation license will also be sent to your mail address." The form contains several input fields: "First name:", "Last name:", "Company:", "Mail:", and "Phone no:". Below these is a section titled "Select software:" with four options, each with a checkbox: "Identity Manager:", "OTP Server:", "Automatic Account Manager:", and "Secure FTP server:". The "OTP Server:" checkbox is checked and circled in red. A "Send" button is located at the bottom of the form.

You will receive a link for downloading the software. A 30 days evaluation license will be sent via e-mail when you download the software.

Download the version with JAVA included.

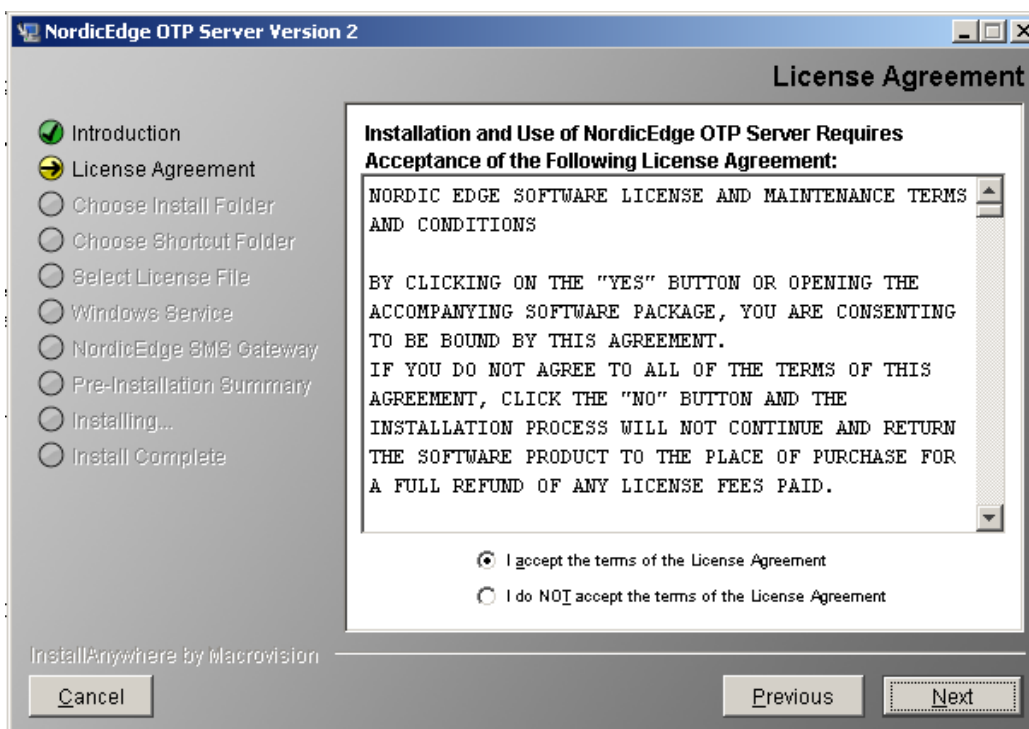
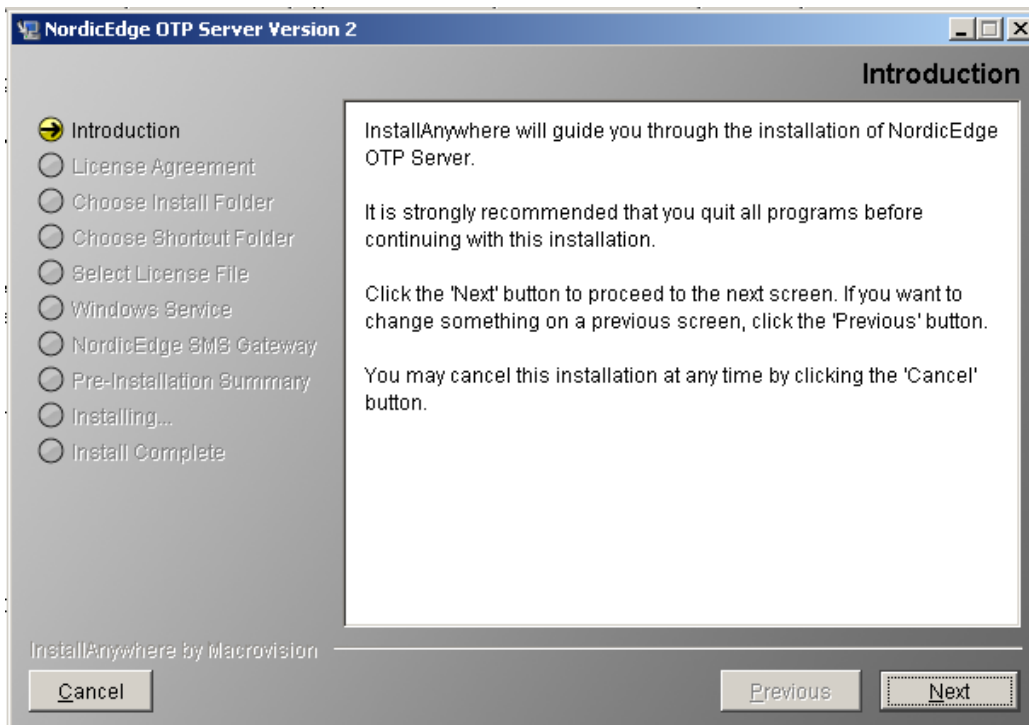


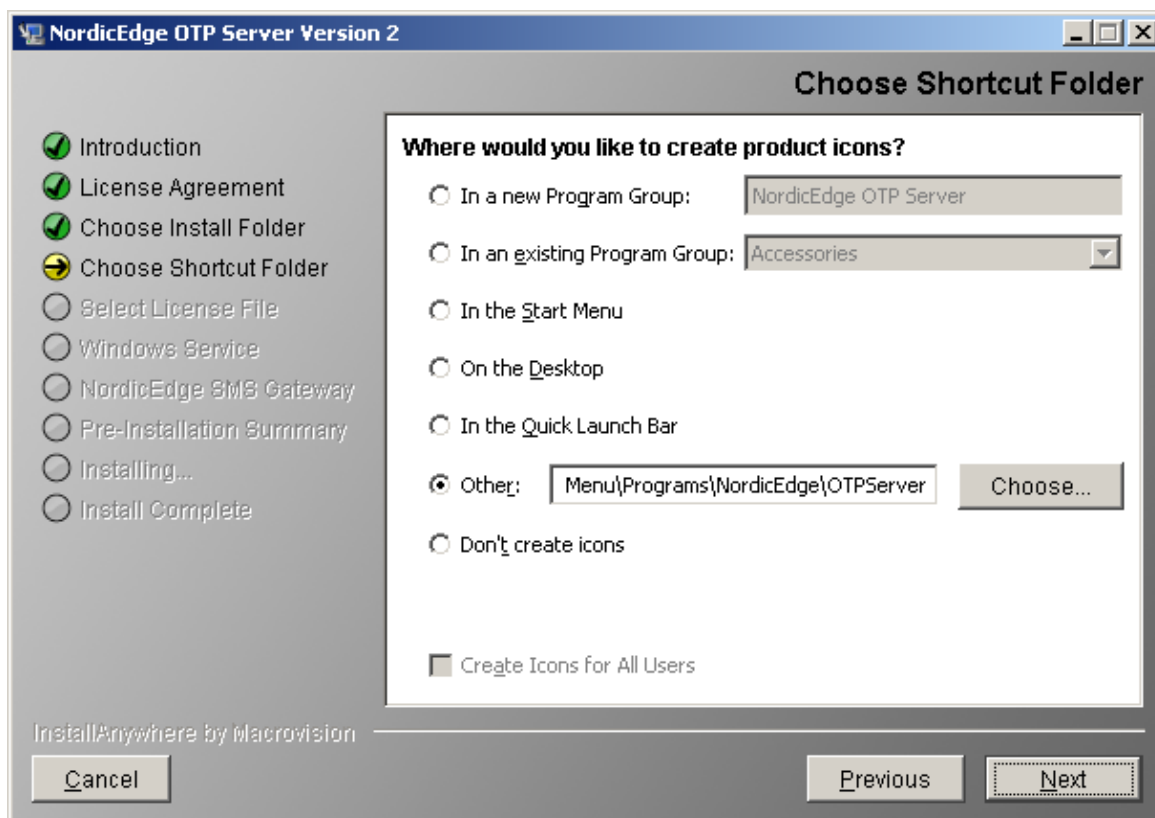
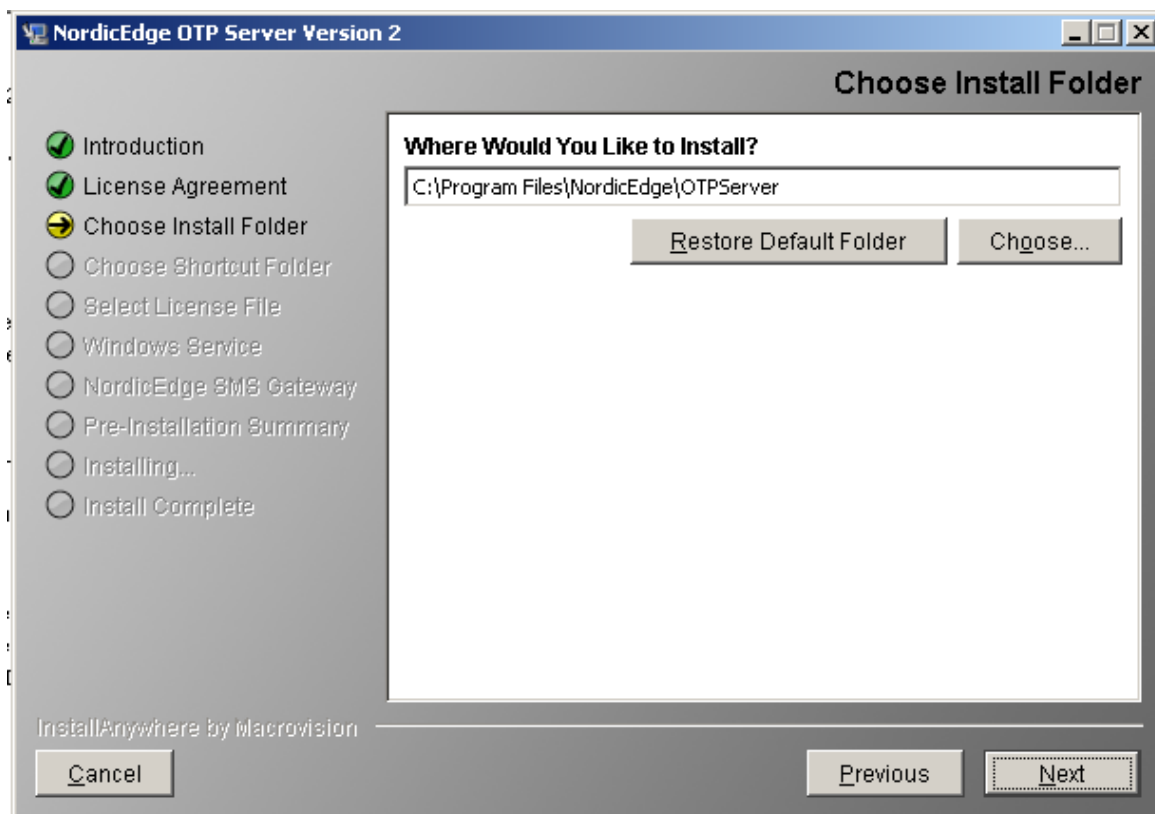


## 5 Installation

### 5.1 Start the installation

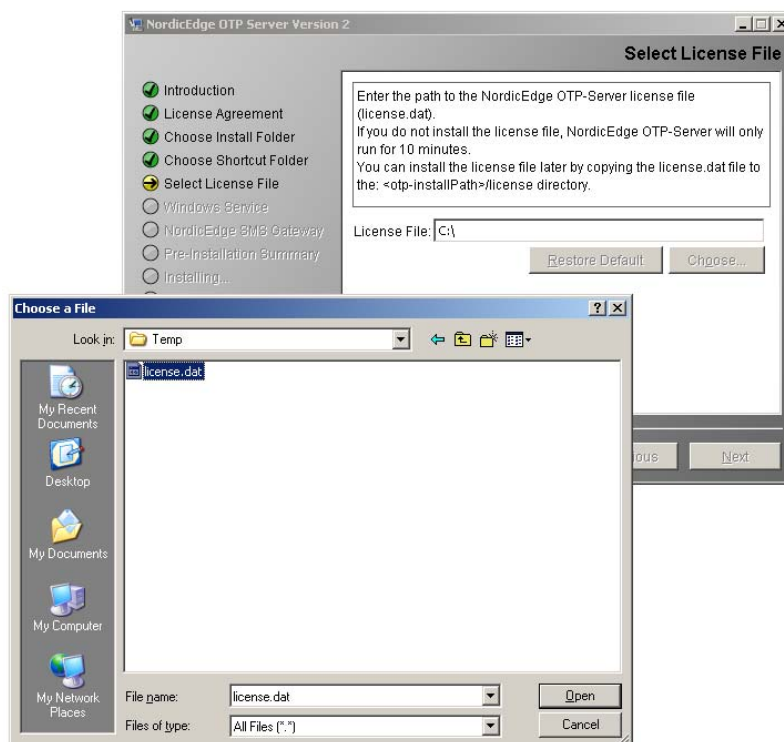
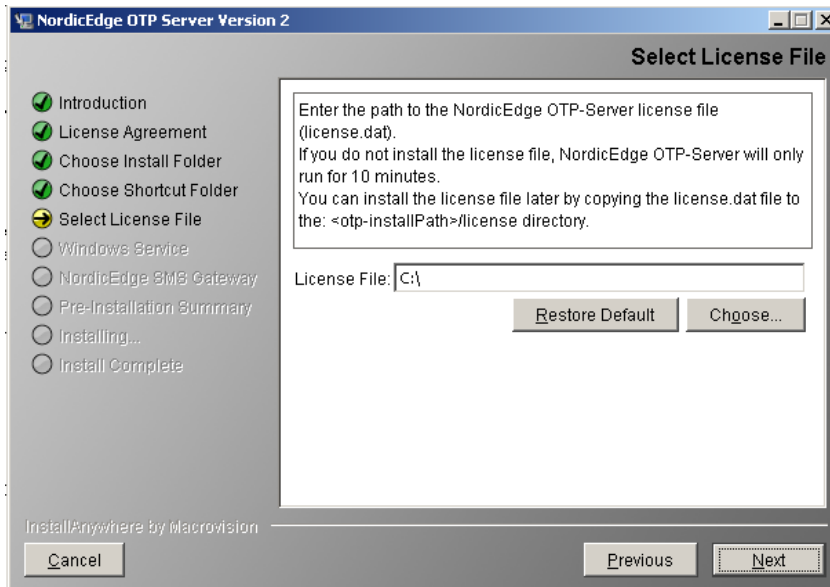
Start the installation on the server where you want to install the One Time Password Server

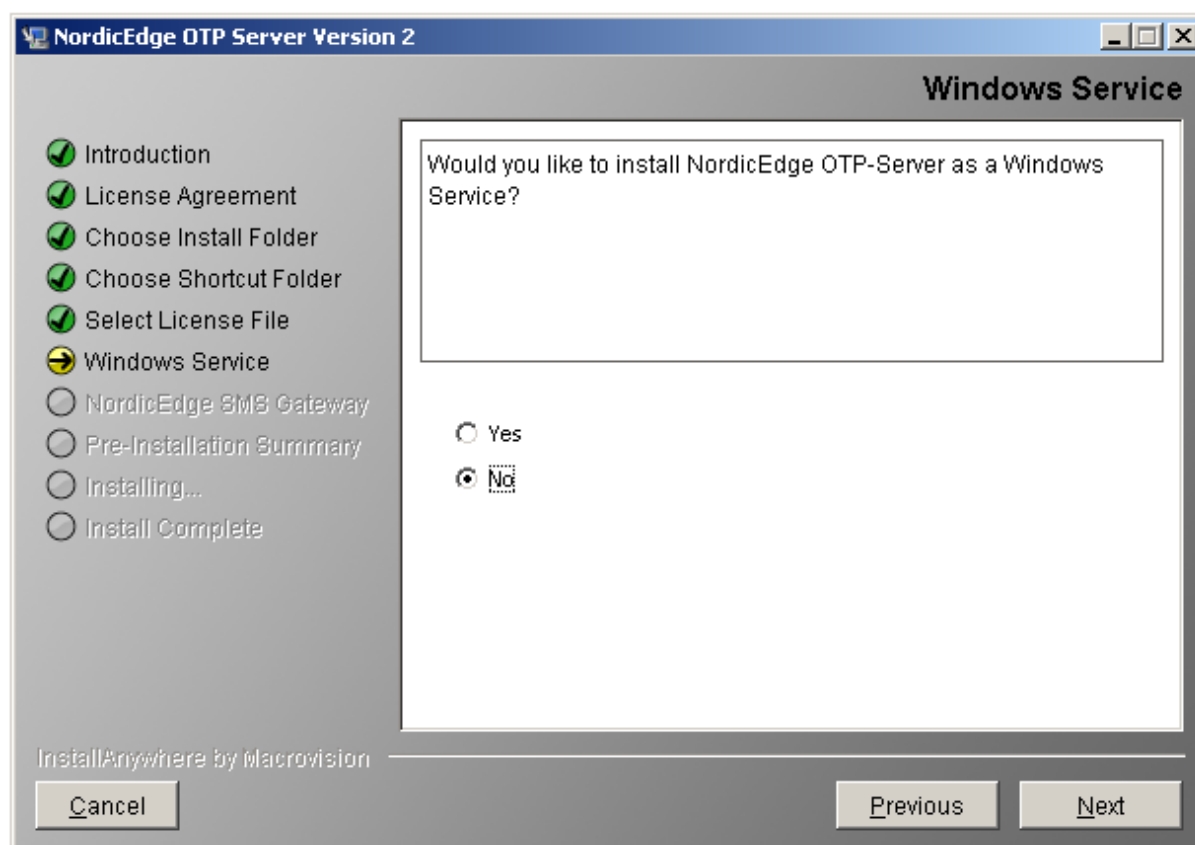




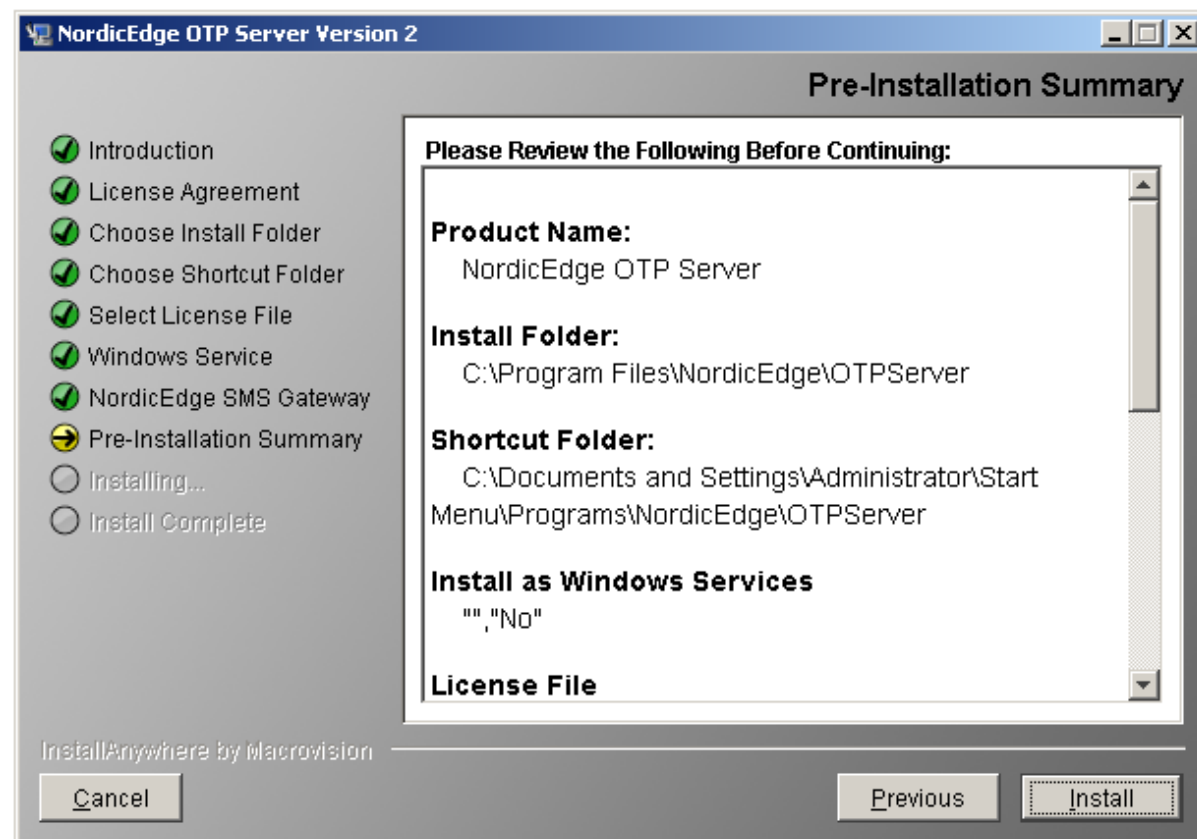
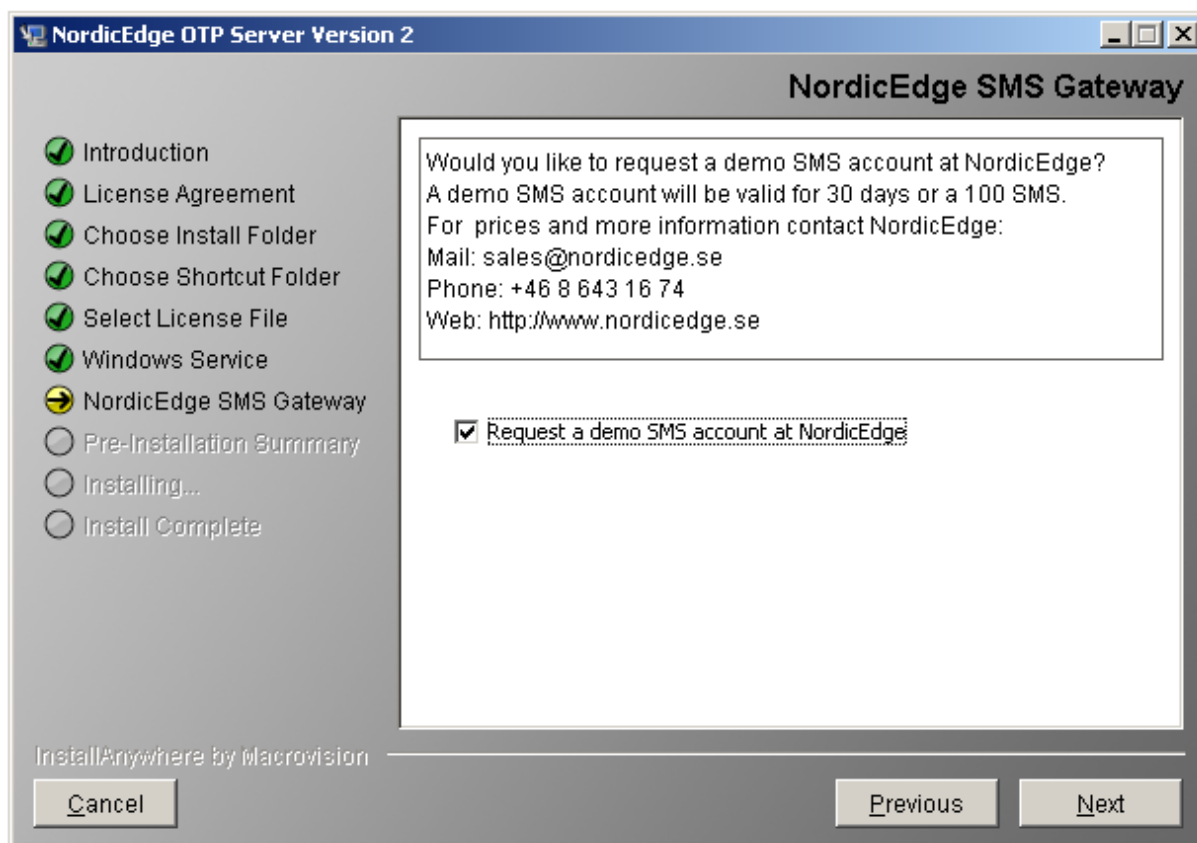
## 5.2 Installing license

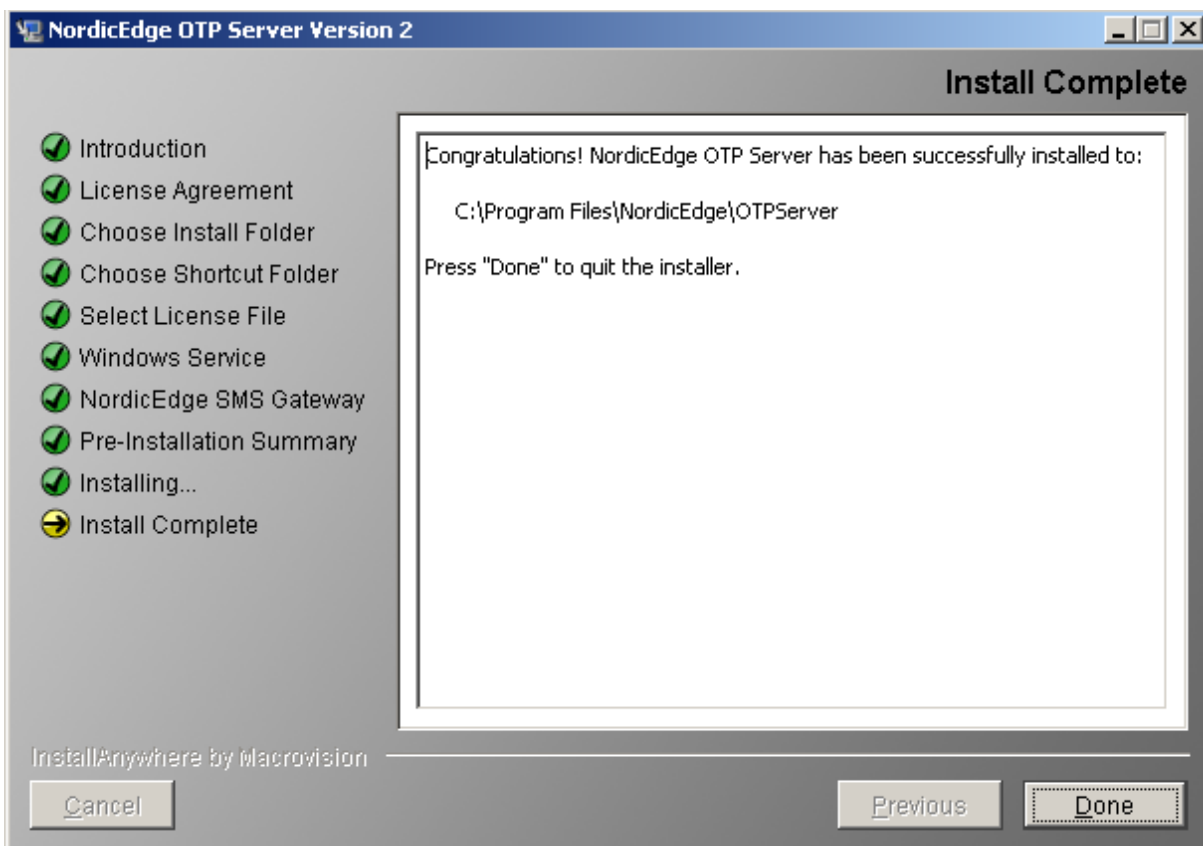
Choose the license.dat that you have received via e-mail. This is important, since if you want to request a demo SMS account at Nordic Edge later in the installation, you need to install the license at this moment.





Note, if you are in a test-phase, we recommend that you do not install the OTP-Server as a Windows Service.

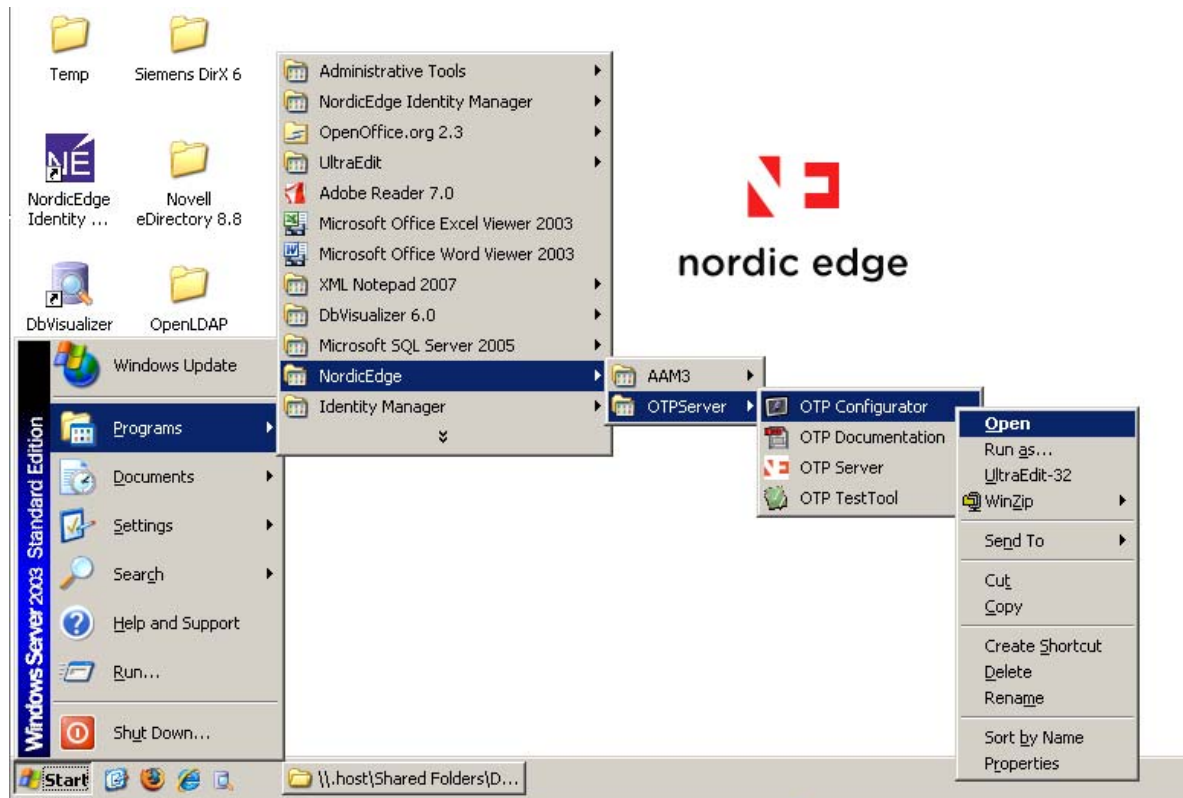




## 6 Configuring the One Time Password Server

### 6.1 Start the OTP Configuration

Start the OTP Configurator by clicking on Programs / NordicEdge / OTP Configurator

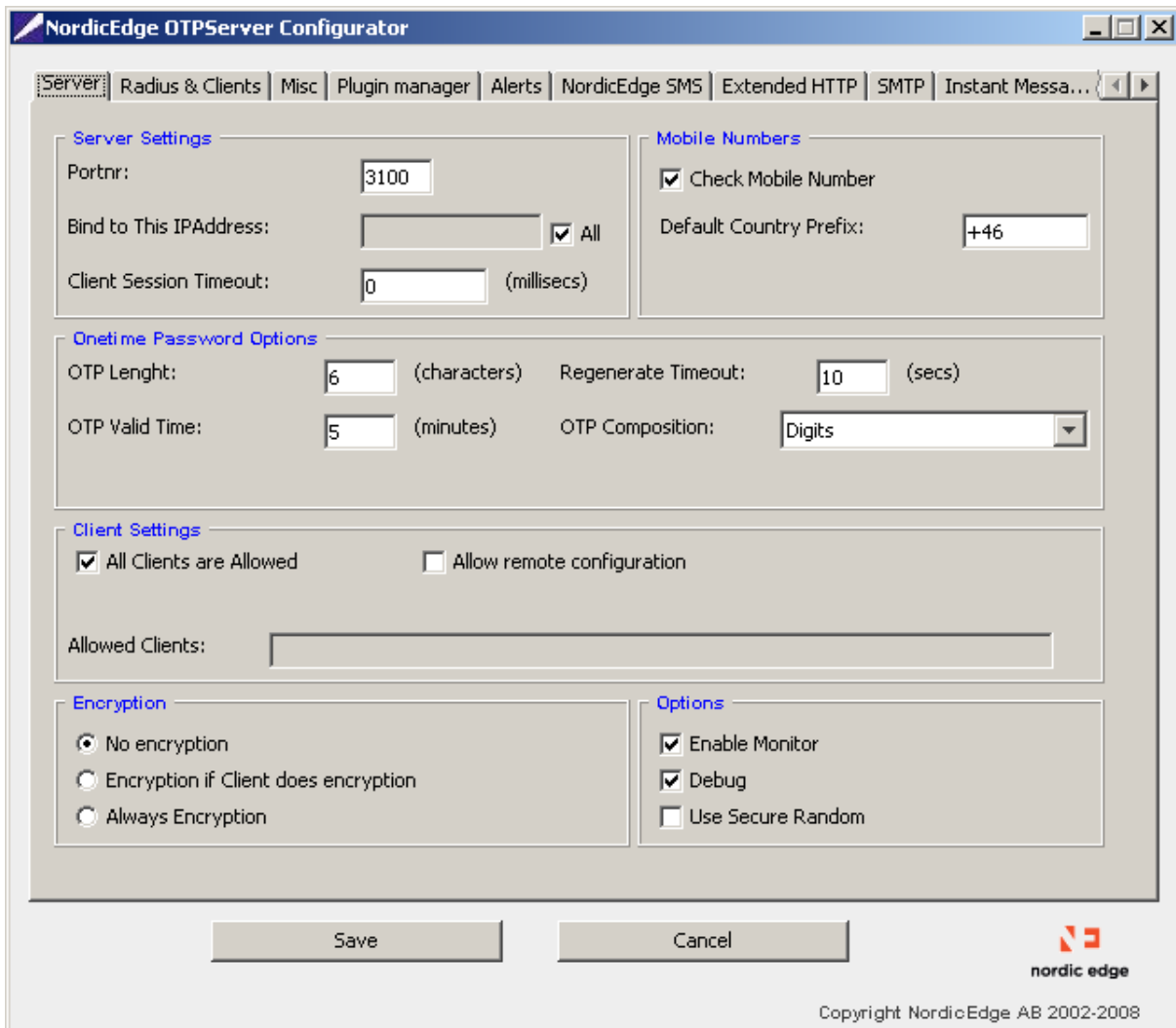


## 6.2 Server page

On the Server page you can set the length of the one-time password and for how long it should be valid. Default is 5 minutes.

You can also set a default country prefix, which means that you will not need to state it in the mobile attribute.

The One Time Password communicates with TCP protocol portnr 3100.



The screenshot shows the 'NordicEdge OTPServer Configurator' window with the 'Server' tab selected. The window has a tabbed interface with tabs for 'Server', 'Radius & Clients', 'Misc', 'Plugin manager', 'Alerts', 'NordicEdge SMS', 'Extended HTTP', 'SMTP', and 'Instant Messa...'. The 'Server' tab contains several sections:

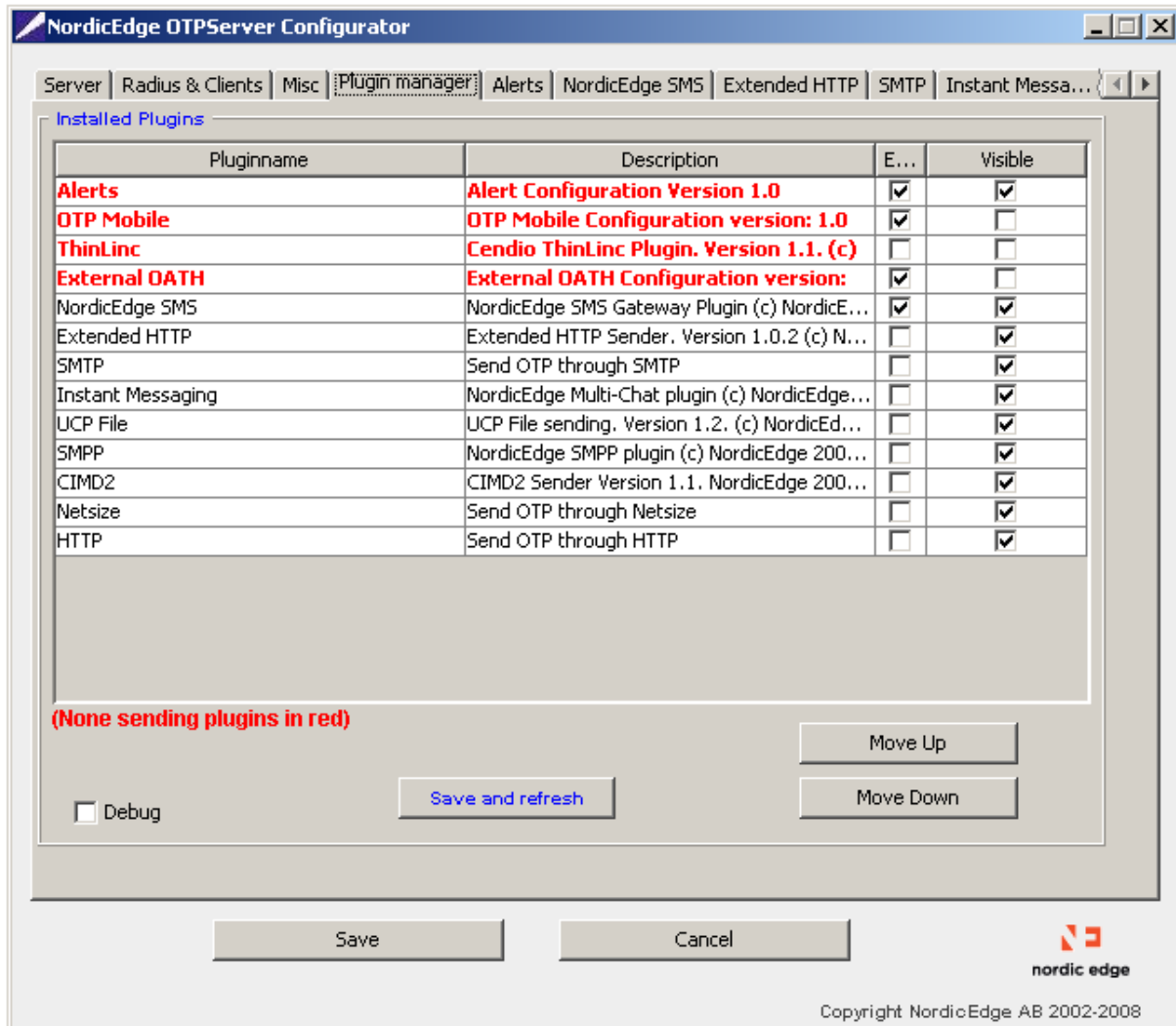
- Server Settings:** Portnr: 3100; Bind to This IPAddress: [ ] All; Client Session Timeout: 0 (milliseconds).
- Mobile Numbers:** Check Mobile Number (checked); Default Country Prefix: +46.
- Onetime Password Options:** OTP Length: 6 (characters); Regenerate Timeout: 10 (secs); OTP Valid Time: 5 (minutes); OTP Composition: Digits (dropdown).
- Client Settings:** All Clients are Allowed (checked); Allow remote configuration (unchecked); Allowed Clients: [ ].
- Encryption:** No encryption (selected), Encryption if Client does encryption, Always Encryption.
- Options:** Enable Monitor (checked), Debug (checked), Use Secure Random (unchecked).

At the bottom, there are 'Save' and 'Cancel' buttons. The footer includes the Nordic Edge logo, the text 'Copyright NordicEdge AB 2002-2008', and the website 'www.nordicedge.se'.



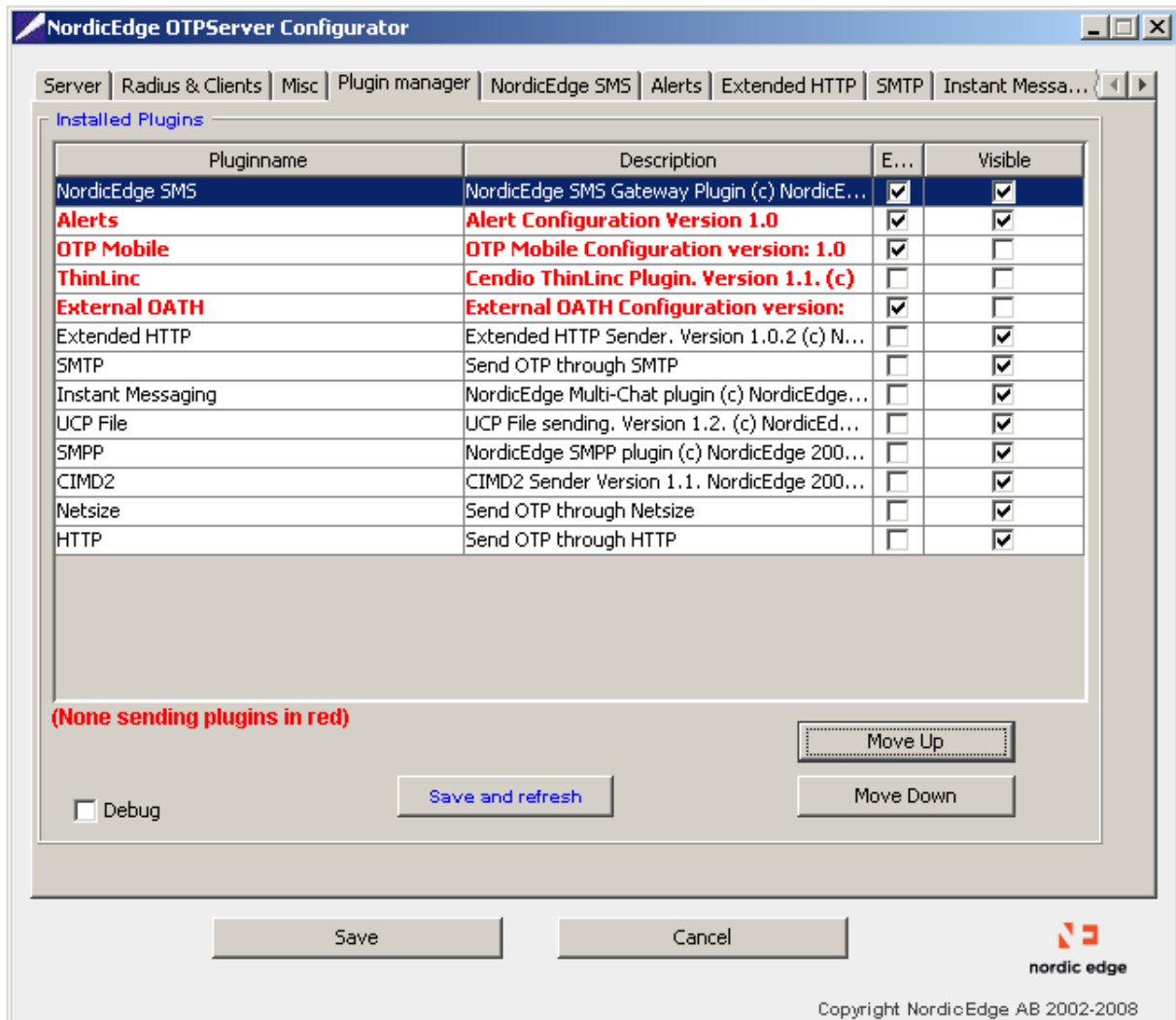
### 6.3 Plugin manager page

On the Plugin manager page you can configure all methods and in which order you want to use them. In this case we will be using Nordic Edge SMS gateway to deliver the one-time password via SMS to your mobile phone.



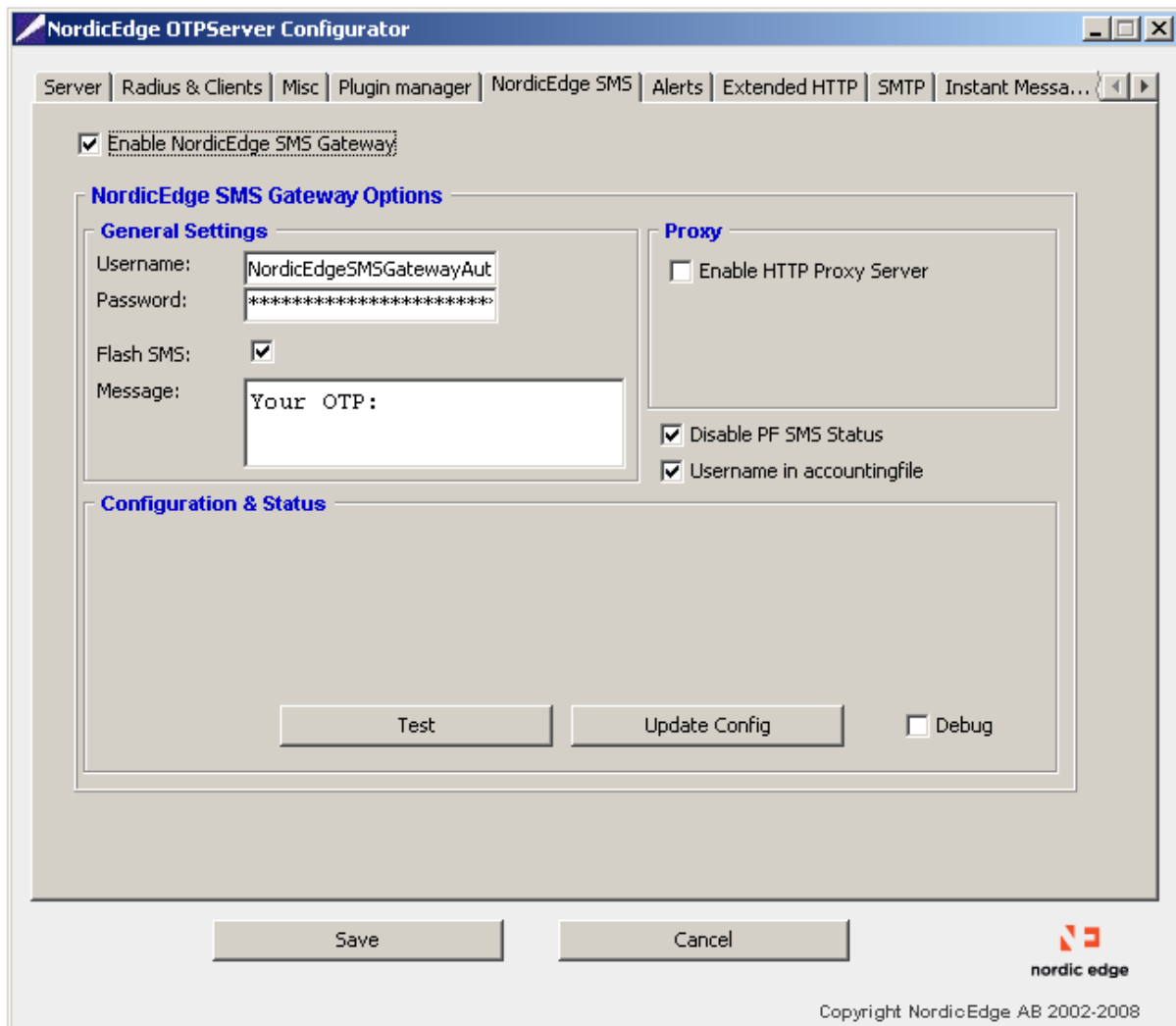
### 6.3.1 Nordic Edge SMS Plugin

Move the Plugin Nordic Edge SMS to the top of the plugins.



## 6.4 Nordic Edge SMS Page

Look at the Nordic Edge SMS Page. If you installed the license.dat during the installation and checked the box "Request a demo SMS account at Nordic Edge", an account should now be preconfigured for you.



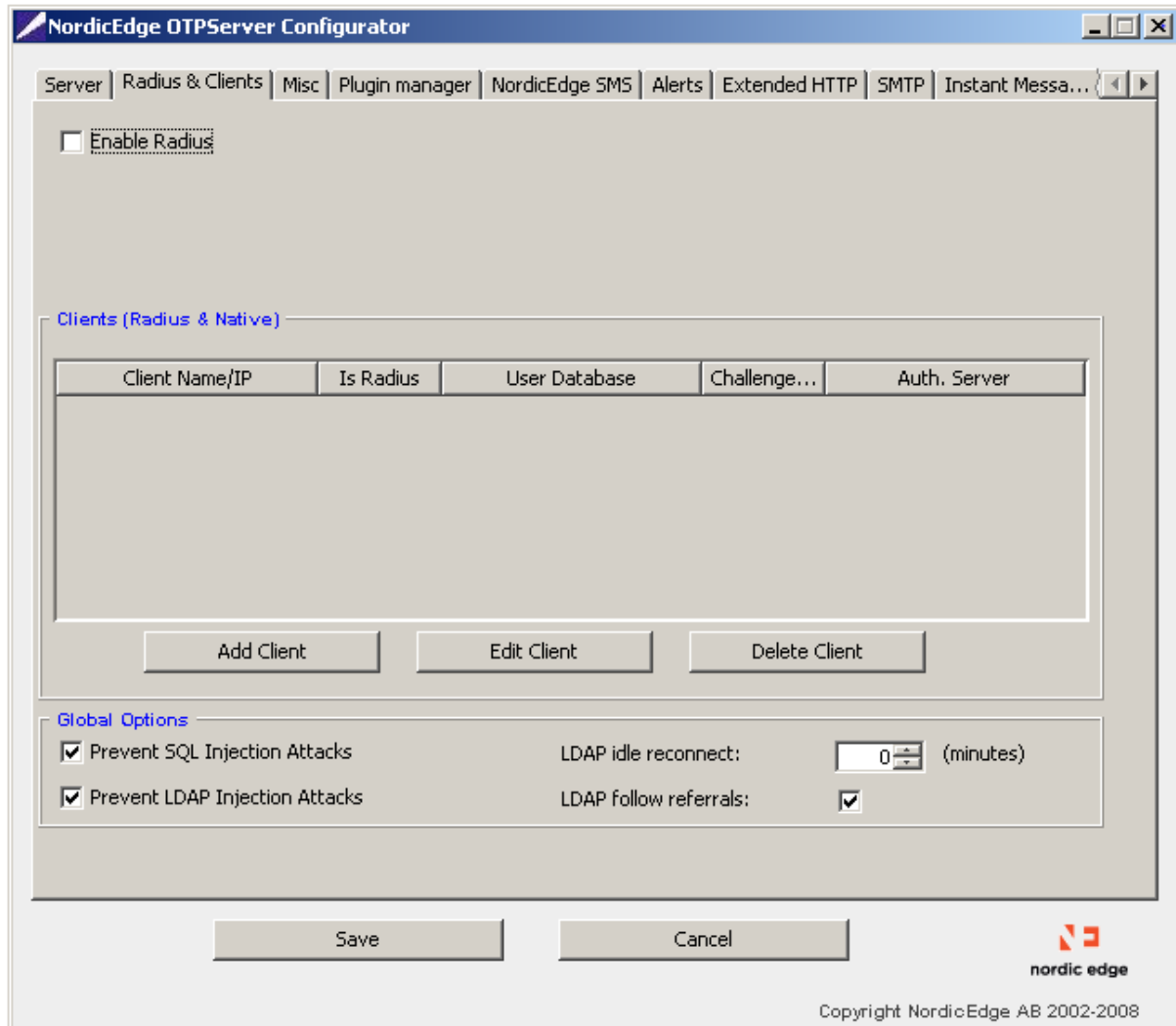
The screenshot shows the "NordicEdge OTPServer Configurator" window with the "NordicEdge SMS" tab selected. The window has a menu bar with options: Server, Radius & Clients, Misc, Plugin manager, NordicEdge SMS, Alerts, Extended HTTP, SMTP, and Instant Messa... The main content area is divided into sections:

- Enable NordicEdge SMS Gateway:** A checkbox that is checked.
- NordicEdge SMS Gateway Options:**
  - General Settings:**
    - Username: NordicEdgeSMSTGatewayAut
    - Password: \*\*\*\*\*
    - Flash SMS: ☒
    - Message: Your OTP :
  - Proxy:**
    - Enable HTTP Proxy Server: ☐
    - Disable PF SMS Status: ☒
    - Username in accountingfile: ☒
- Configuration & Status:**
  - Buttons: Test, Update Config, Debug (checkbox)

At the bottom of the window are "Save" and "Cancel" buttons. The Nordic Edge logo and "Copyright NordicEdge AB 2002-2008" are in the bottom right corner.

## 6.5 Radius & Client page

For configuring One Time Passwords Server to act as radius server go to the Radius & Client page.



The screenshot shows the 'NordicEdge OTPServer Configurator' window with the 'Radius & Clients' tab selected. The window has a menu bar with options: Server, Radius & Clients, Misc, Plugin manager, NordicEdge SMS, Alerts, Extended HTTP, SMTP, and Instant Messa... The main content area includes an 'Enable Radius' checkbox, which is currently unchecked. Below this is a section titled 'Clients (Radius & Native)' containing a table with the following headers: Client Name/IP, Is Radius, User Database, Challenge..., and Auth. Server. The table is currently empty. Below the table are three buttons: 'Add Client', 'Edit Client', and 'Delete Client'. At the bottom of the main content area is a 'Global Options' section with four settings: 'Prevent SQL Injection Attacks' (checked), 'Prevent LDAP Injection Attacks' (checked), 'LDAP idle reconnect:' (set to 0 minutes), and 'LDAP follow referrals:' (checked). At the bottom of the window are 'Save' and 'Cancel' buttons. The Nordic Edge logo and copyright information 'Copyright NordicEdge AB 2002-2008' are in the bottom right corner.

**NordicEdge OTPServer Configurator**

Server | Radius & Clients | Misc | Plugin manager | NordicEdge SMS | Alerts | Extended HTTP | SMTP | Instant Messa...

☐ Enable Radius

Clients (Radius & Native)

Client Name/IP	Is Radius	User Database	Challenge...	Auth. Server
----------------	-----------	---------------	--------------	--------------


Add Client Edit Client Delete Client

Global Options

☒ Prevent SQL Injection Attacks ☐ LDAP idle reconnect: 0 (minutes)

☒ Prevent LDAP Injection Attacks ☒ LDAP follow referrals:

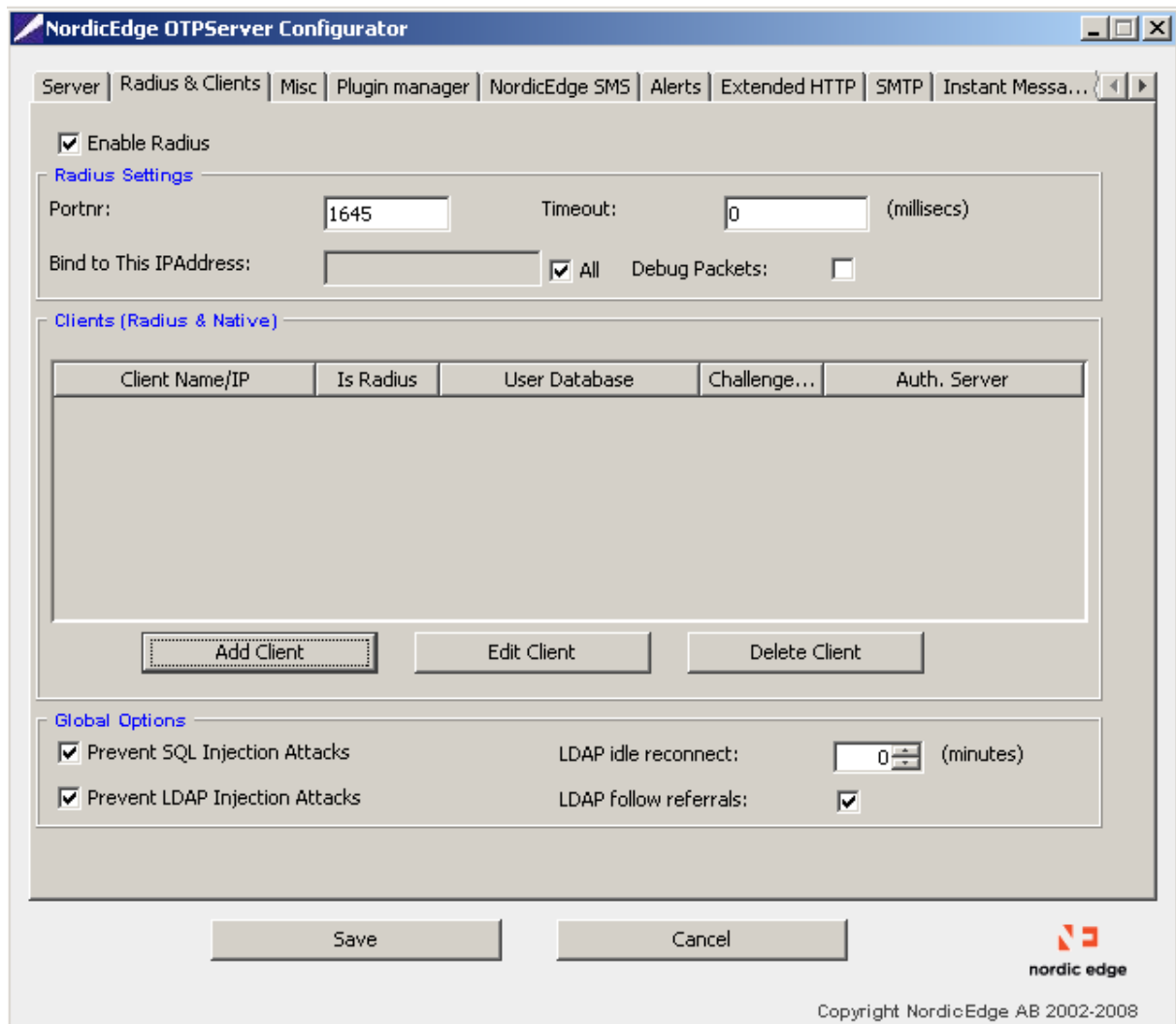
Save Cancel

 nordic edge

Copyright NordicEdge AB 2002-2008

## 6.5.1 Enable Radius

Enable Radius and choose one of the radius ports 1645 or 1812 that you want to use. Make sure that the client (Cisco 5500 ASA) is using the same radius port.



The screenshot shows the 'NordicEdge OTPServer Configurator' window with the 'Radius & Clients' tab selected. The 'Enable Radius' checkbox is checked. Under 'Radius Settings', the 'Portnr:' is set to 1645 and 'Timeout:' is 0 (milliseconds). The 'Bind to This IPAddress:' field is empty, and the 'All' checkbox is checked. The 'Debug Packets:' checkbox is unchecked. Below this is a table for 'Clients (Radius & Native)' with columns: Client Name/IP, Is Radius, User Database, Challenge..., and Auth. Server. The table is currently empty. Below the table are buttons for 'Add Client', 'Edit Client', and 'Delete Client'. Under 'Global Options', 'Prevent SQL Injection Attacks' and 'Prevent LDAP Injection Attacks' are checked. 'LDAP idle reconnect:' is set to 0 (minutes) and 'LDAP follow referrals:' is checked. At the bottom are 'Save' and 'Cancel' buttons. The Nordic Edge logo and copyright notice 'Copyright NordicEdge AB 2002-2008' are at the bottom right.

**NordicEdge OTPServer Configurator**

Server | Radius & Clients | Misc | Plugin manager | NordicEdge SMS | Alerts | Extended HTTP | SMTP | Instant Messa...

☒ Enable Radius

**Radius Settings**

Portnr: 1645 Timeout: 0 (milliseconds)

Bind to This IPAddress:  ☒ All Debug Packets: ☐

**Clients (Radius & Native)**

Client Name/IP	Is Radius	User Database	Challenge...	Auth. Server
----------------	-----------	---------------	--------------	--------------


Add Client Edit Client Delete Client

**Global Options**

☒ Prevent SQL Injection Attacks LDAP idle reconnect: 0 (minutes)

☒ Prevent LDAP Injection Attacks LDAP follow referrals: ☒

Save Cancel

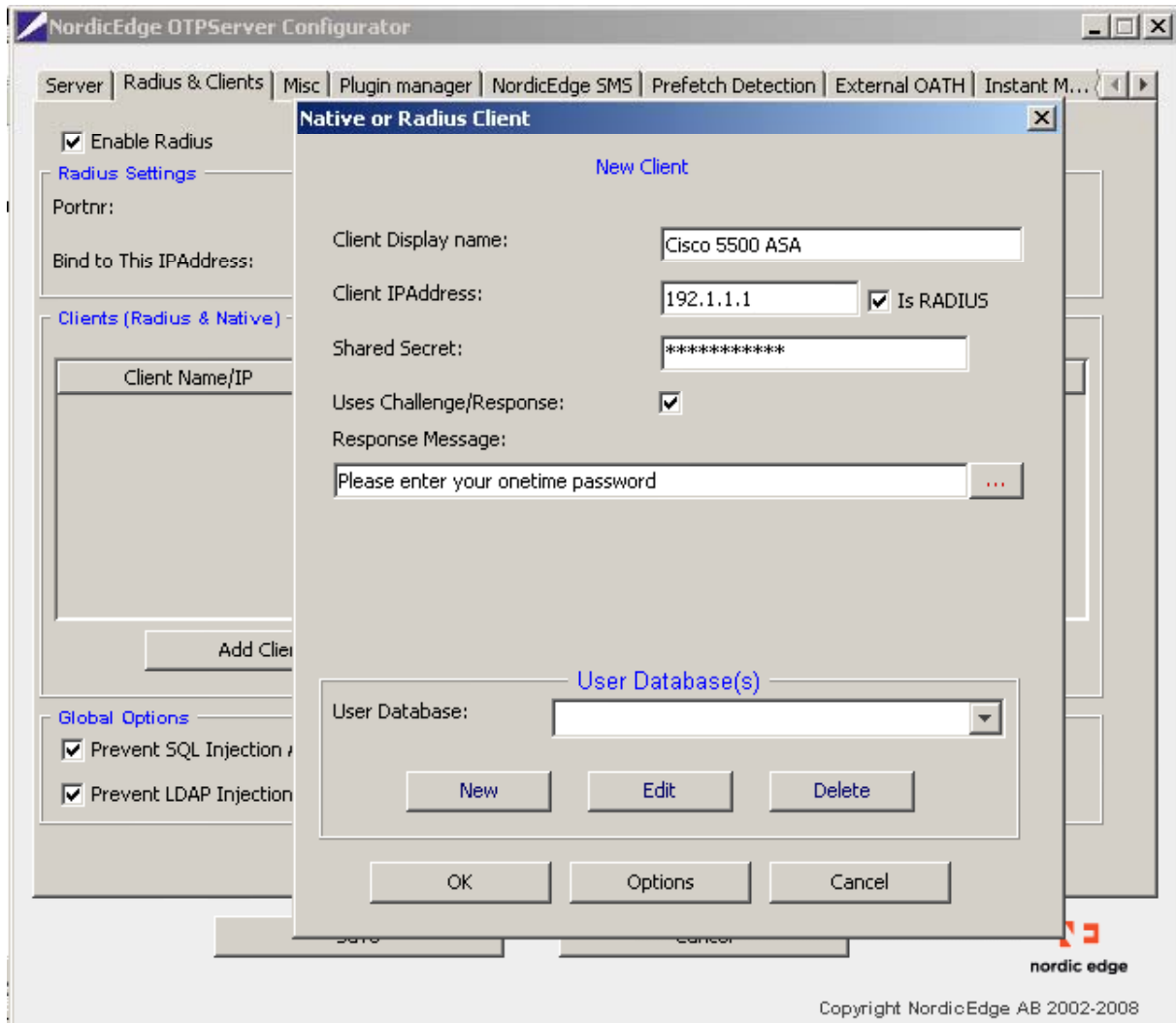
 nordic edge

Copyright NordicEdge AB 2002-2008

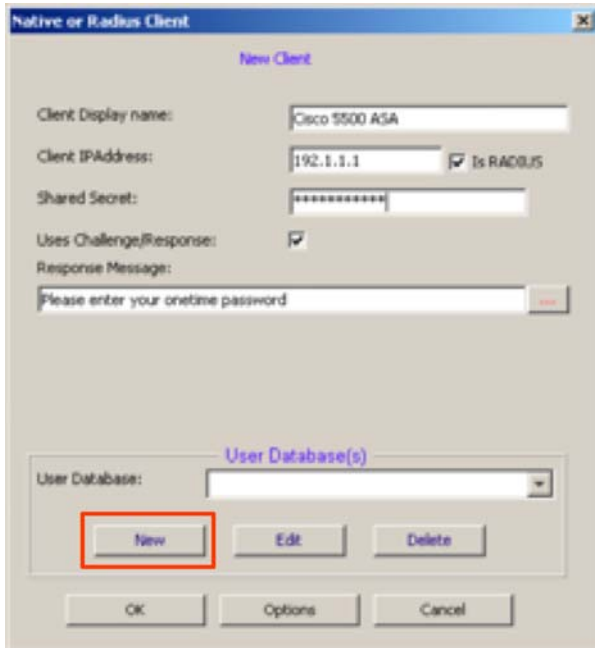
## 6.6 Add client

Click on Add Client and enter Client Display name and the ip-address for the Cisco 5500 ASA. Please note that you should not use the hostname here.

Make sure that "Is RADIUS" is checked and enter the correct Shared Secret.



In the category User Database (s) click New.



## 6.7 Configure LDAP

Enter a Database Display Name and the host address for your LDAP user database. In this case we are using Microsoft Active Directory with SSL and the users' mobile attribute for sending one time passwords.

### 6.7.1 Test LDAP Connection

Click on Test LDAP Connection and make sure that you get an LDAP Connection Success.

**New User Database**

Database Display Name:  Database Type:

☐ Database is for OTP Mobile/Card users only!

**LDAP** | **JDBC** | **Database Group**

**Host Settings**

Host Address:

Portnumber:  ☒ SSL ☐ TLS

Admin DN:

Password:

**Account Settings**

OTP Attribute:

Login Retries:  ☐ Accept Pwd change

Inactive Attribute:

Inactive Value:

Disable OTP Attribute:

Disable OTP Value:  ☐ Not

Search Base DN:

Search Scope:

Search Filter Start:

Search Filter End:

**Onetime Password Prefetch**

☐ Enable OTP Prefetch

**Pin code**

☐ Enable Pin Code

**Advanced options**

☐ External Databasehandler



## 6.7.2 Selecting Search Base DN

Click on the box for selecting Search Base DN:

**New User Database**

Database Display Name:  Database Type: **LDAP**

☐ **Database is for OTP Mobile/Card users only!**

**LDAP** | JDBC | Database Group

**Host Settings**

Host Address:

Portnumber:  ☒ SSL ☐ TLS

Admin DN:

Password:

**Account Settings**

OTP Attribute:  ...

Login Retries:  ☐ Accept Pwd change

Inactive Attribute:  ...

Inactive Value:

Disable OTP Attribute:  ...

Disable OTP Value:  ☐ Not

**Search Settings**

Search Base DN:  ...

Search Scope: **SUB**

Nr of Connections:

Search Filter Start:

Search Filter End:

**Onetime Password Prefetch**

☐ Enable OTP Prefetch

**Pin code**

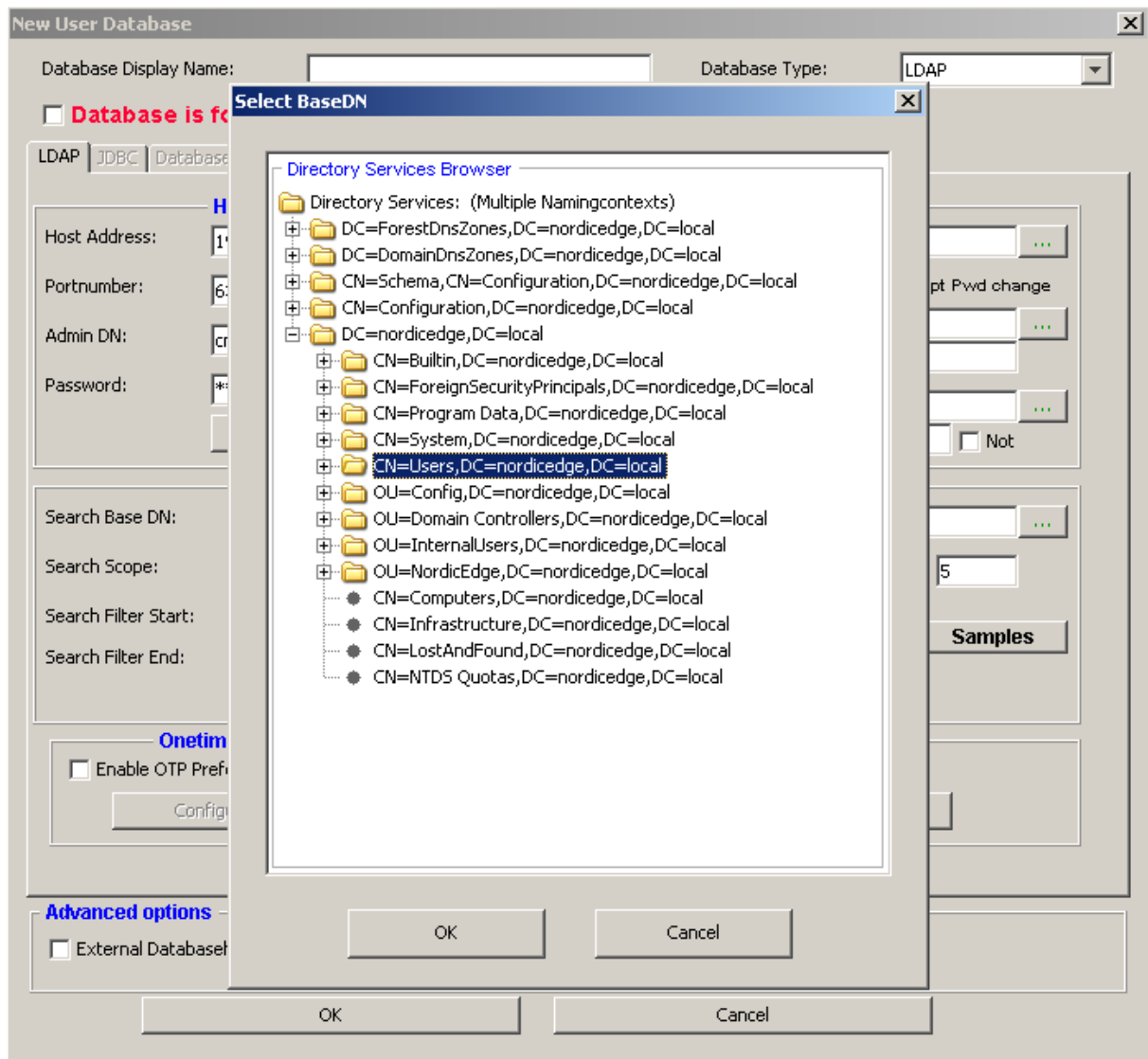
☐ Enable Pin Code

**Advanced options**

☐ External Databasehandler

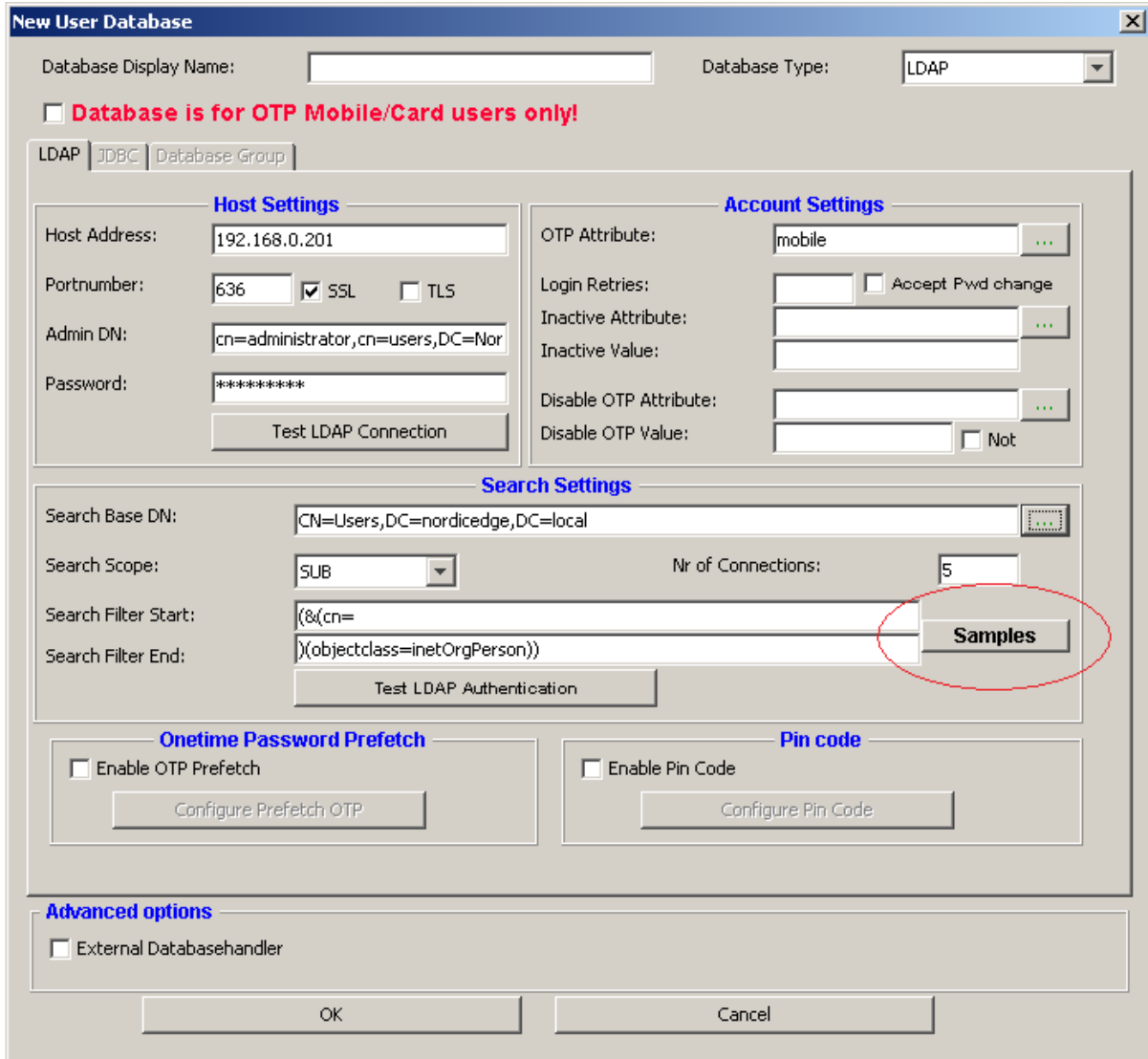


Select a Base Dn where your users are.



### 6.7.3 Select Search filter

Click on samples and select the right filter for your LDAP User database, in this case Active Directory.



**New User Database**

Database Display Name:  Database Type: **LDAP**

☐ **Database is for OTP Mobile/Card users only!**

**LDAP** | JDBC | Database Group

**Host Settings**

Host Address:

Portnumber:  ☒ SSL ☐ TLS

Admin DN:

Password:

**Account Settings**

OTP Attribute:  ...

Login Retries:  ☐ Accept Pwd change

Inactive Attribute:  ...

Inactive Value:

Disable OTP Attribute:  ...

Disable OTP Value:  ☐ Not

**Search Settings**

Search Base DN:  ...

Search Scope: **SUB** Nr of Connections:

Search Filter Start:

Search Filter End:

**Onetime Password Prefetch**

☐ Enable OTP Prefetch

**Pin code**

☐ Enable Pin Code

**Advanced options**

☐ External Databasehandler

**New User Database**

Database Display Name:  Database Type: **LDAP**

☐ **Database is for OTP Mobile/Card users only!**

**LDAP** | JDBC | Database Group

**Host Settings**

Host Address:

Portnumber:  ☒ SSL ☐ TLS

Admin DN:

Password:

**Account Settings**

OTP Attribute:

Login Retries:  ☐ Accept Pwd change

Inactive Attribute:

Inactive Value:

Disable OTP Attribute:

☐ Not

Search Base DN:

Search Scope:

Search Filter Start:

**Onetime Password Prefetch**

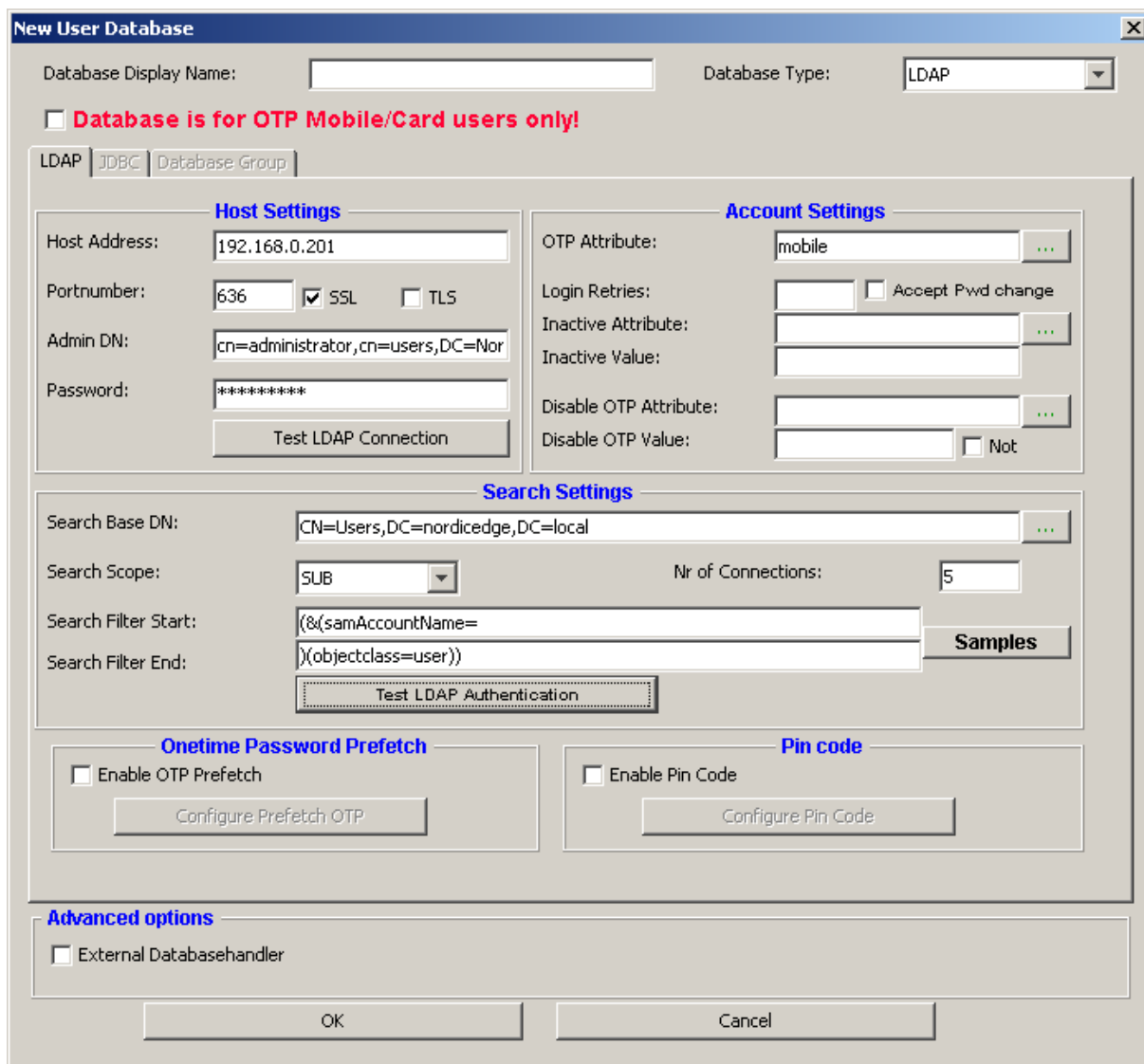
☐ Enable OTP Prefetch

**Pin code**

☐ Enable Pin Code

**Advanced options**

☐ External Databasehandler



**New User Database**

Database Display Name:  Database Type: **LDAP**

☐ **Database is for OTP Mobile/Card users only!**

**LDAP** | JDBC | Database Group

**Host Settings**

Host Address:

Portnumber:  ☒ SSL ☐ TLS

Admin DN:

Password:

**Test LDAP Connection**

**Account Settings**

OTP Attribute:

Login Retries:  ☐ Accept Pwd change

Inactive Attribute:

Inactive Value:

Disable OTP Attribute:

Disable OTP Value:  ☐ Not

**Search Settings**

Search Base DN:

Search Scope: **SUB** Nr of Connections:

Search Filter Start:

Search Filter End:

**Samples**

**Test LDAP Authentication**

**Onetime Password Prefetch**

☐ Enable OTP Prefetch

**Configure Prefetch OTP**

**Pin code**

☐ Enable Pin Code

**Configure Pin Code**

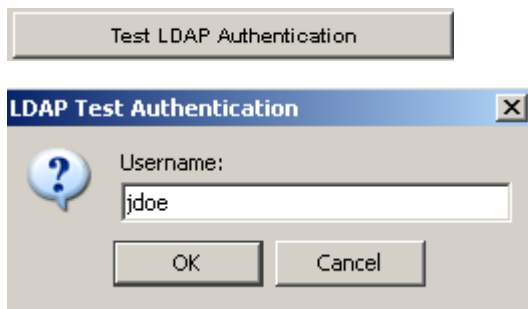
**Advanced options**

☐ External Databasehandler

**OK** **Cancel**

## 6.7.4 Test LDAP Authentication

Click on Test LDAP Authentication and make sure you can authenticate.

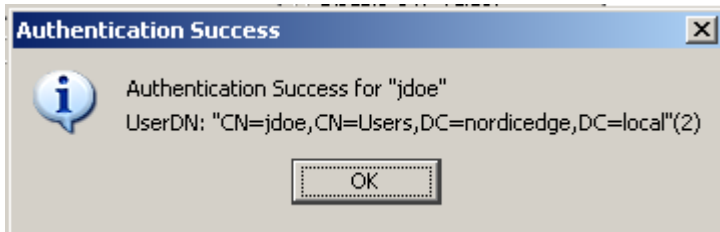


**Test LDAP Authentication**

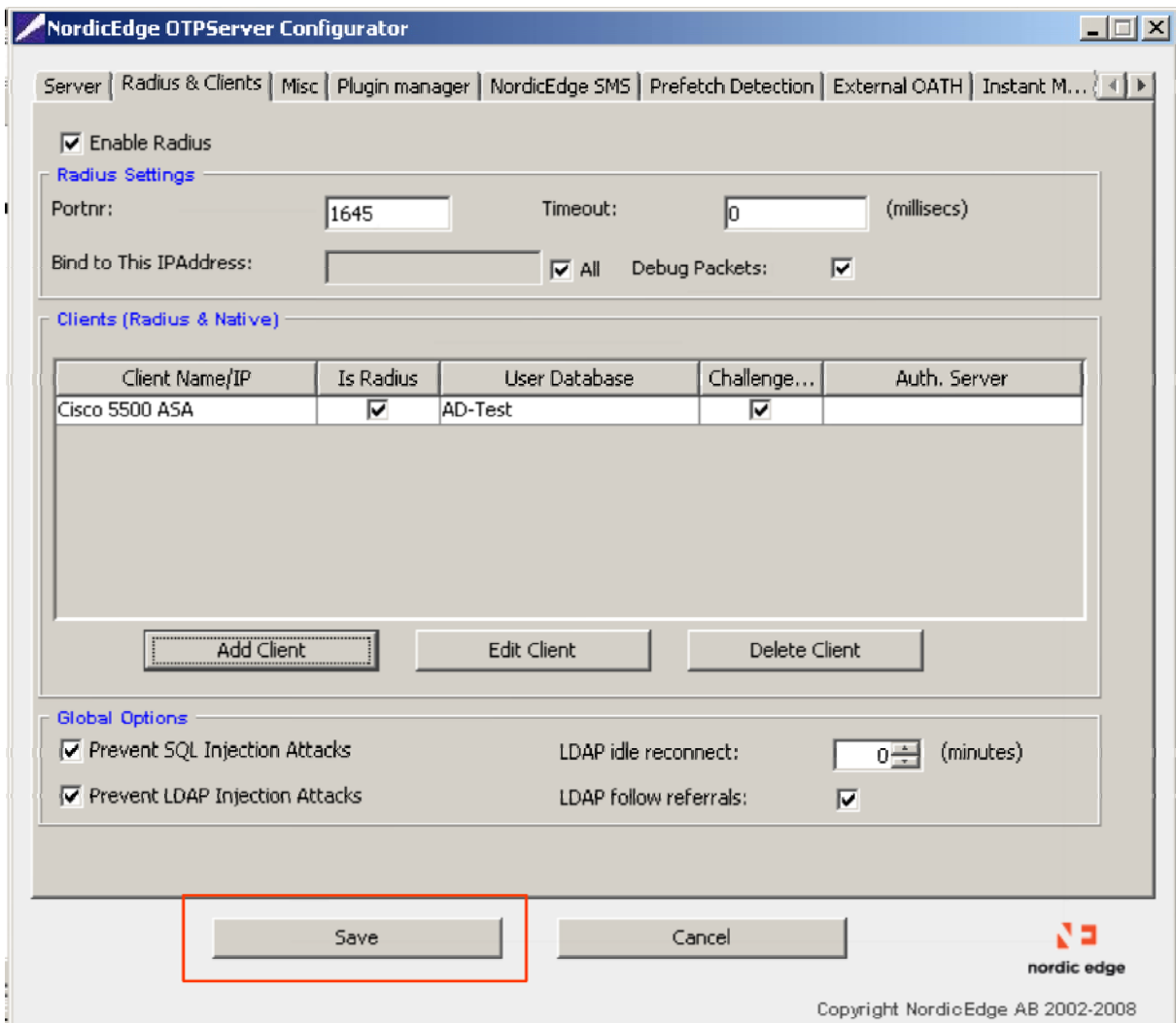
**LDAP Test Authentication**

Username:

**OK** **Cancel**



Exit the configurator by clicking OK twice and make sure to click on the Save button

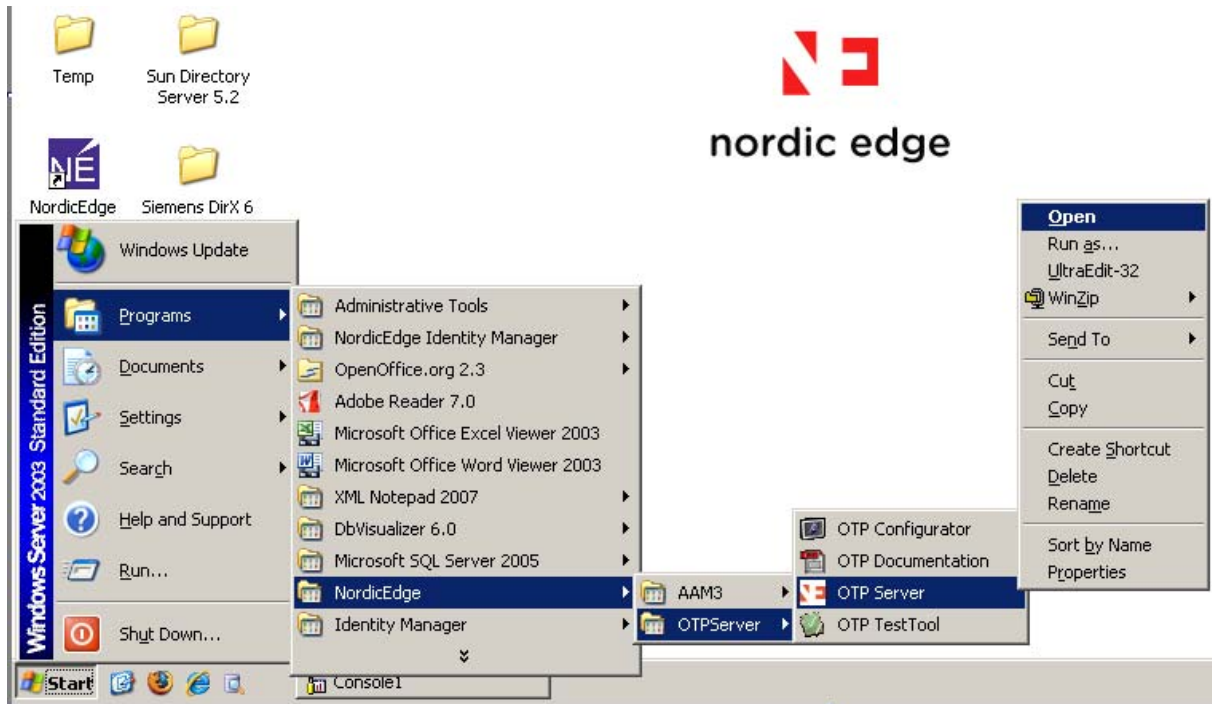


End of Step "Configuring the One Time Password Server"



## 7 Start the One Time Password Server

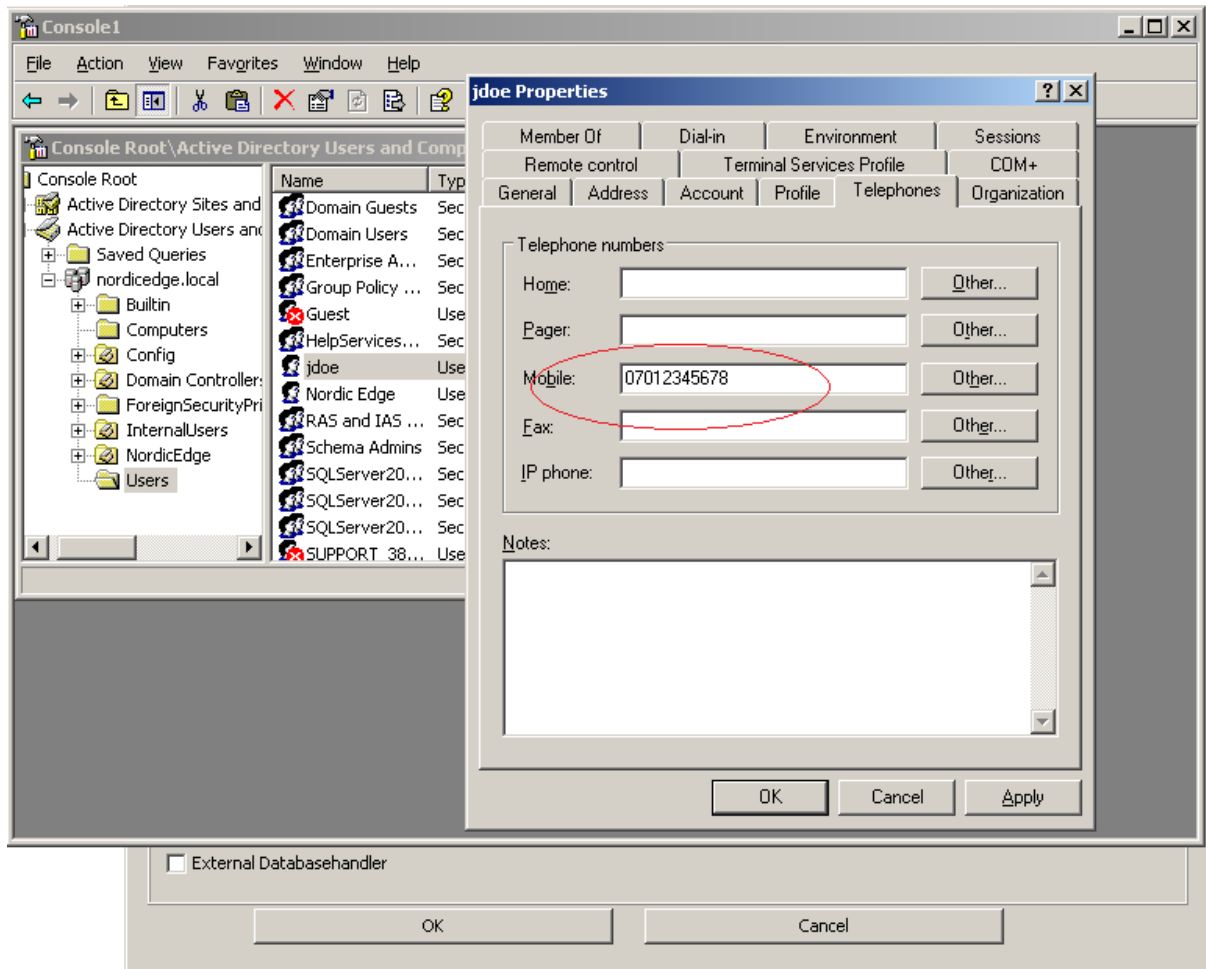
Start the One Time Password by going to Program folder, NordicEdge,OTPServer and click on OTP Server



## 8 Add mobile phone number with Microsoft Management Console

Add mobile phone number to your test users mobile phone attribute

Start MMC and select the user that you want to use for testing and enter the mobile phone number in the Mobile attribute.

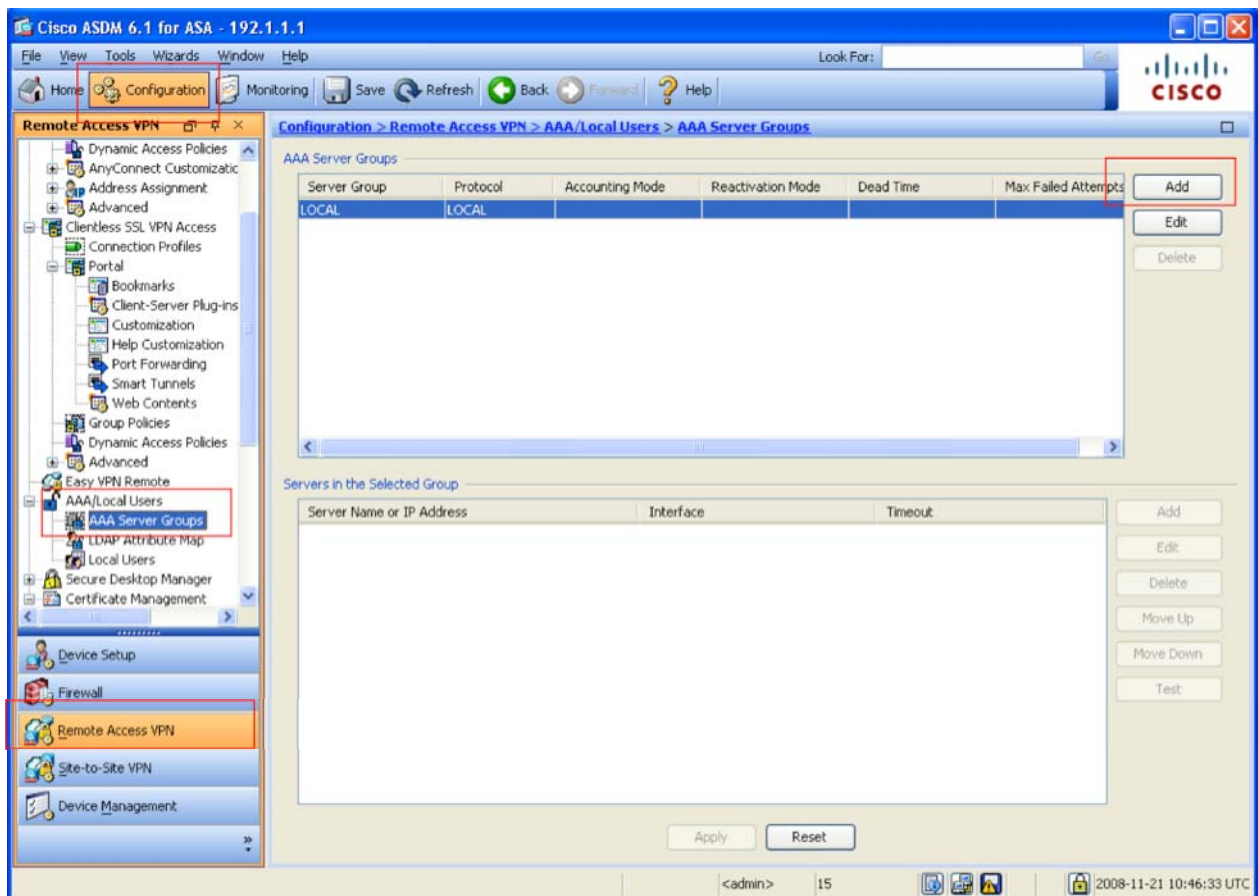




## 9 Configuring ASA5500 for SSL VPN authentication with Nordic Edge One Time Password Server

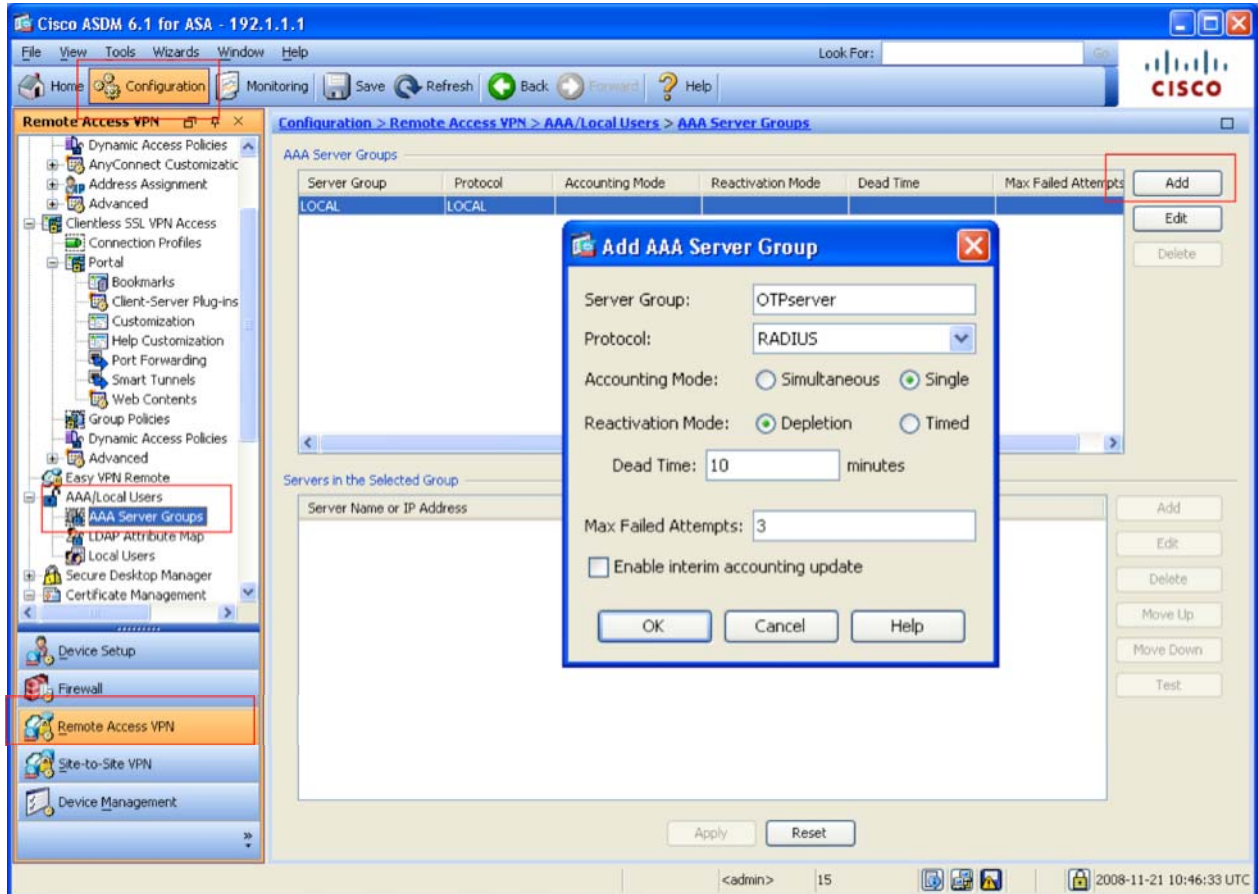
### 9.1 Start ASA device manager

### 9.2 Browse to Configuration, Remote Access VPN, AAA/Local Users, AAA Server Groups and click Add.

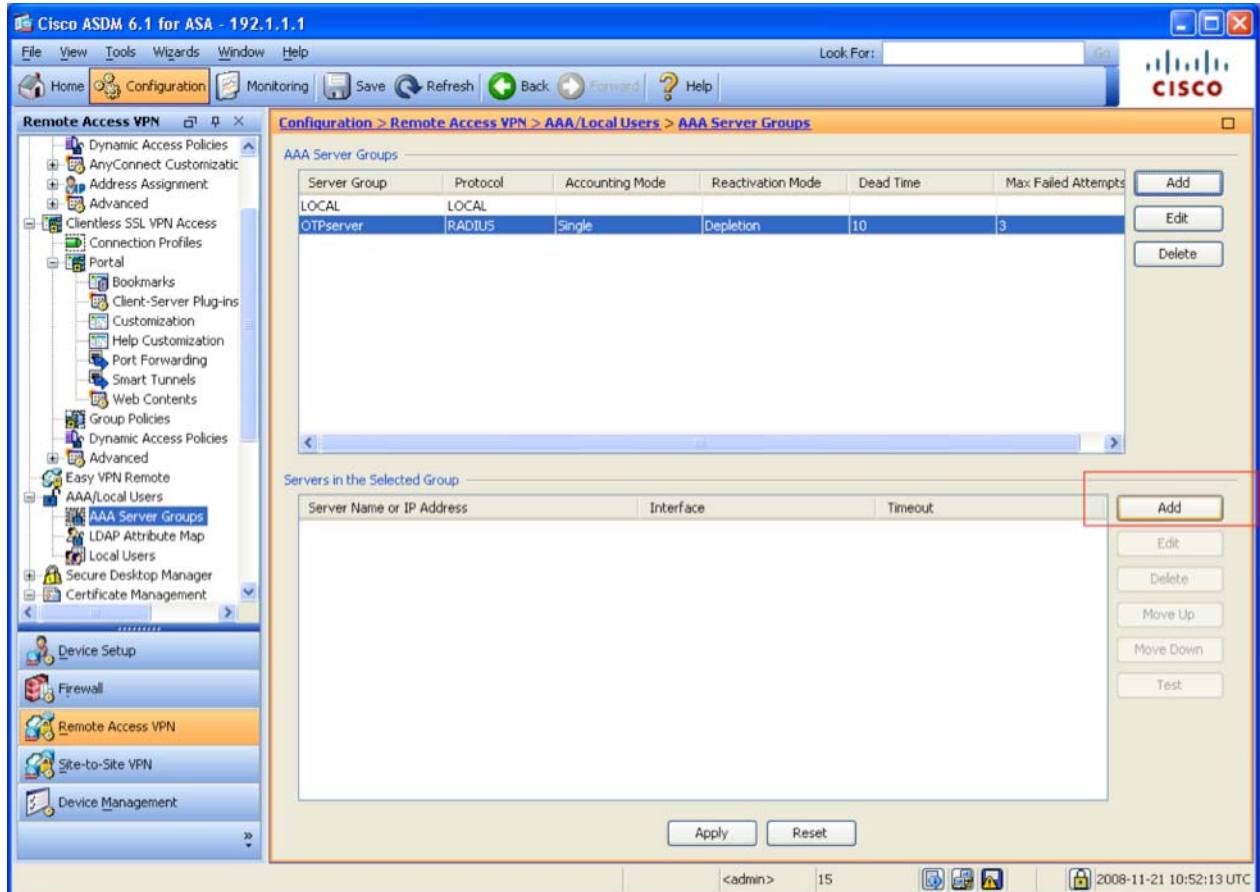




### 9.3 Name Server Group OTPserver, choose protocol RADIUS

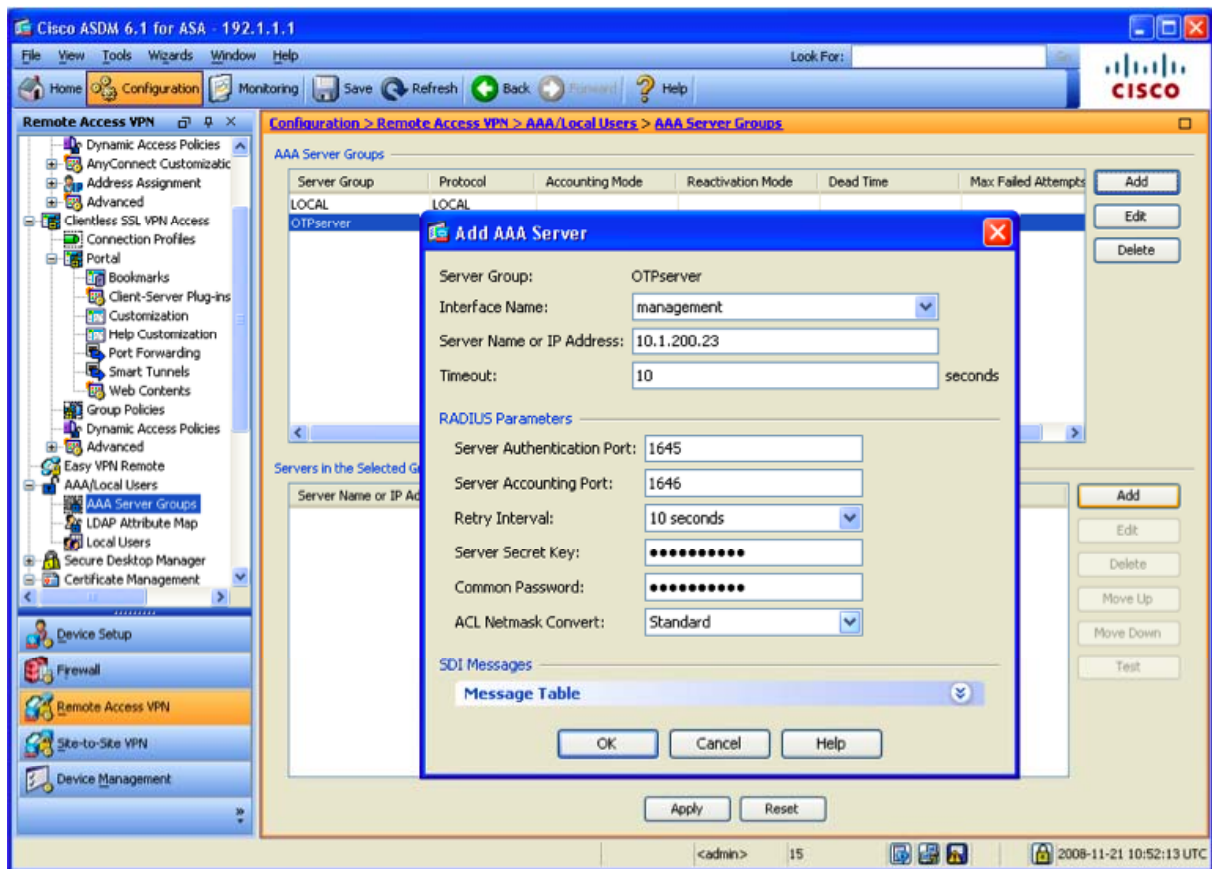


## 9.4 Add new radius server to the RADIUS group



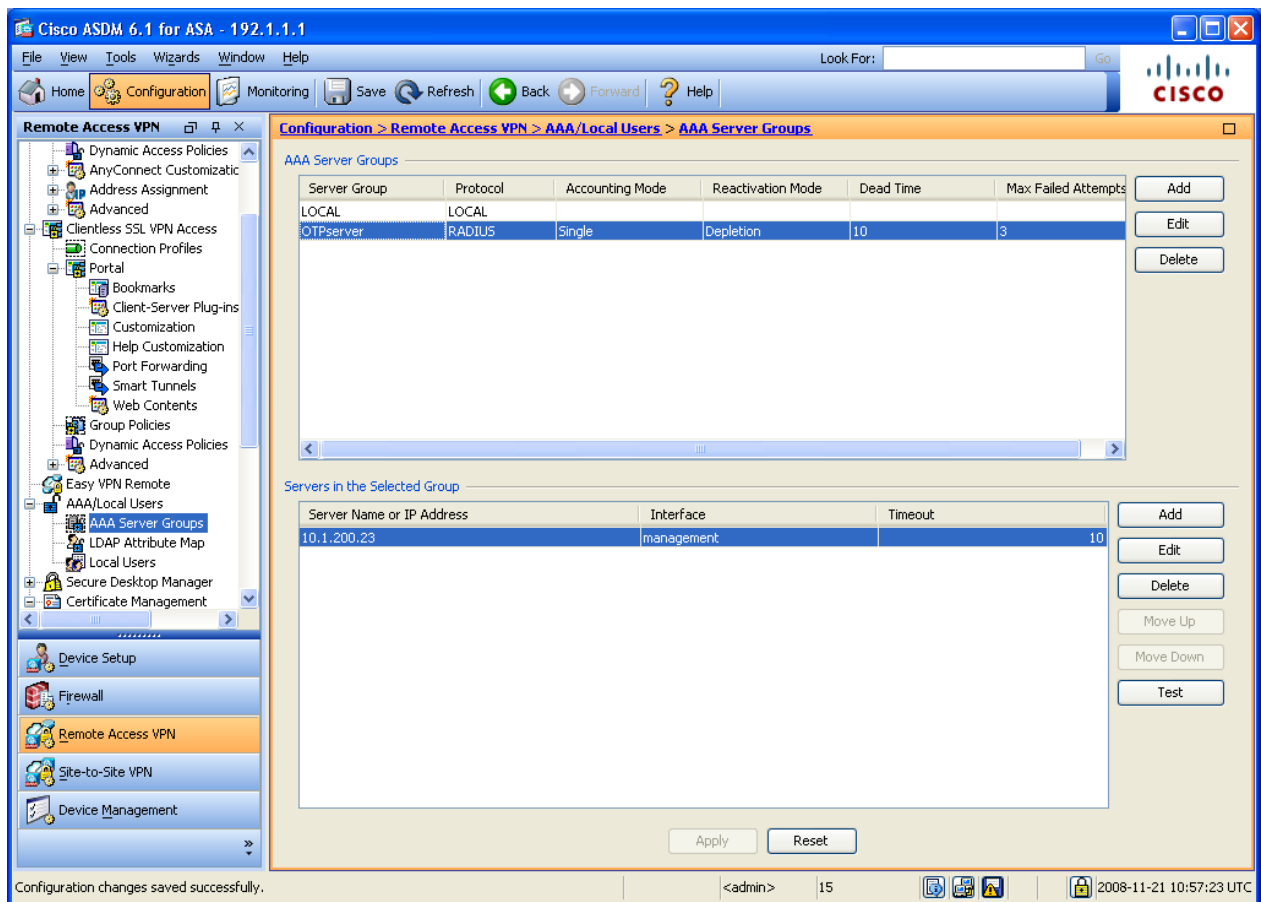
## 9.5 Configure Radius Server : Interface name, IP address to OTPserver and the pre-shared key between the One Time Password server and Cisco ASA5500.

Ensure you use the same radius ports in both OTPserver ASA5500.



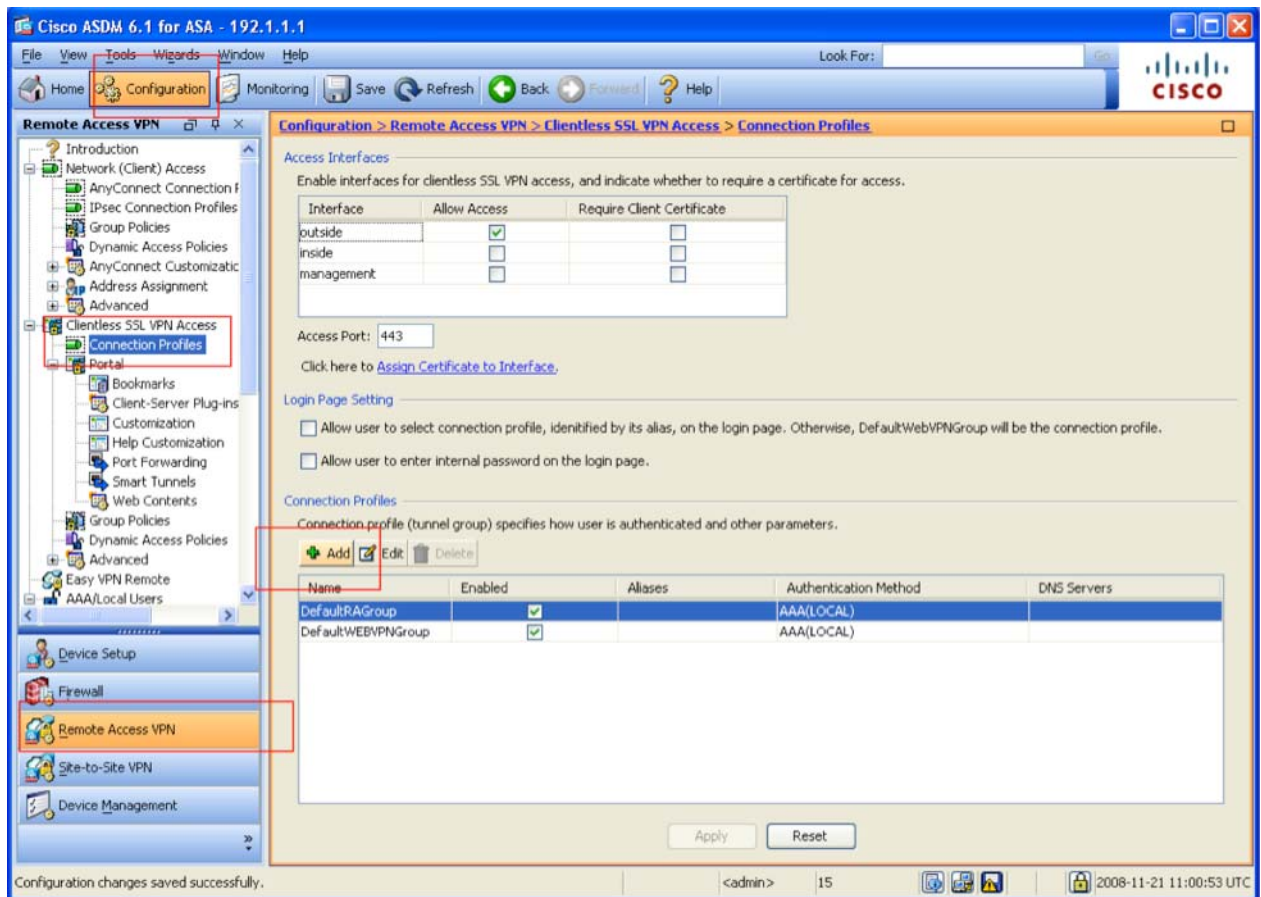
You have now configured a group "OTPserver" and defined a Radius Server in this group.

This group can now be used as an authentication method.



## 9.6 Create a "test" connection profile (in case you want to test this for certain users only).

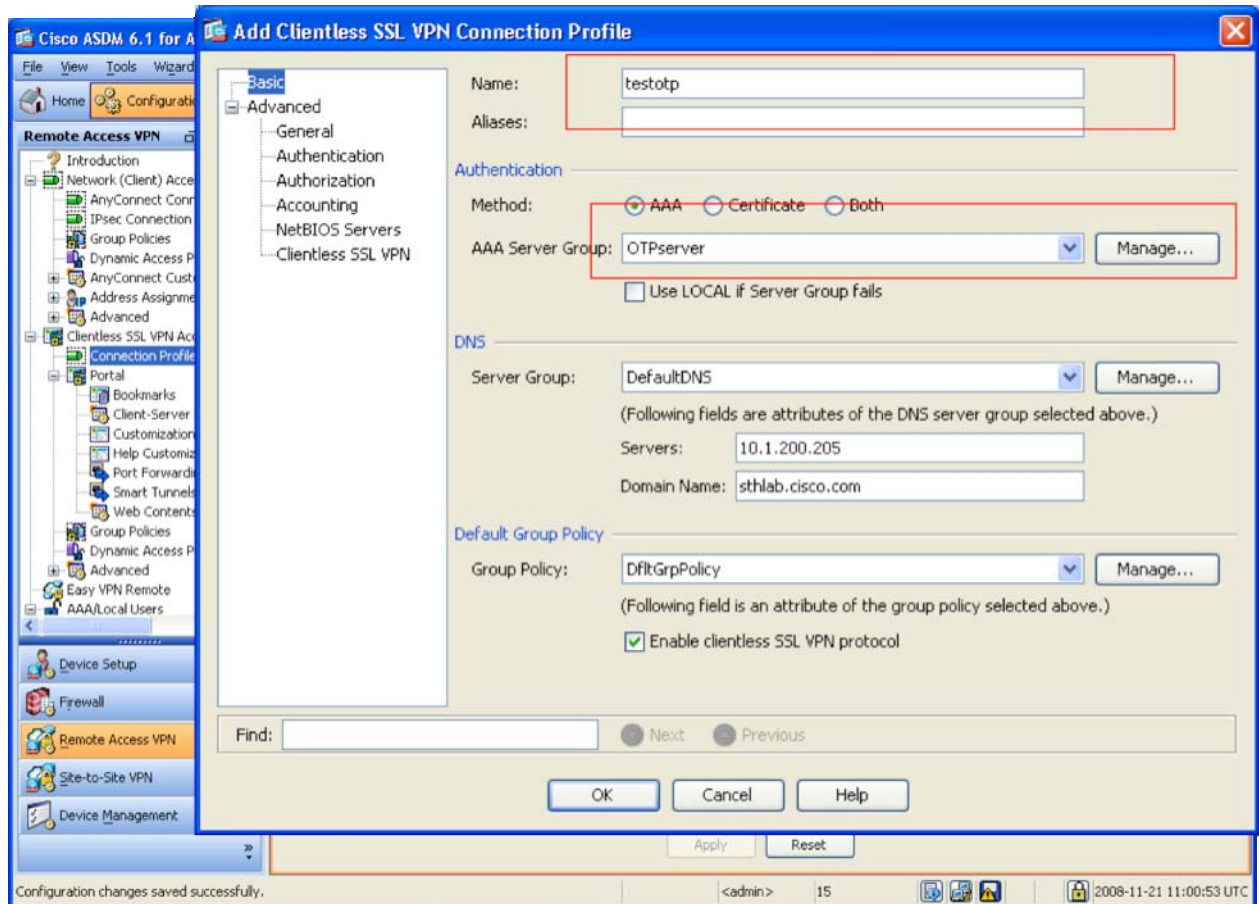
### 9.6.1 Browse to Configuration/Remote Access/Clientless SSL VPN Access/Connection Profiles and click Add



## 9.6.2 Specify Connection Profile Name

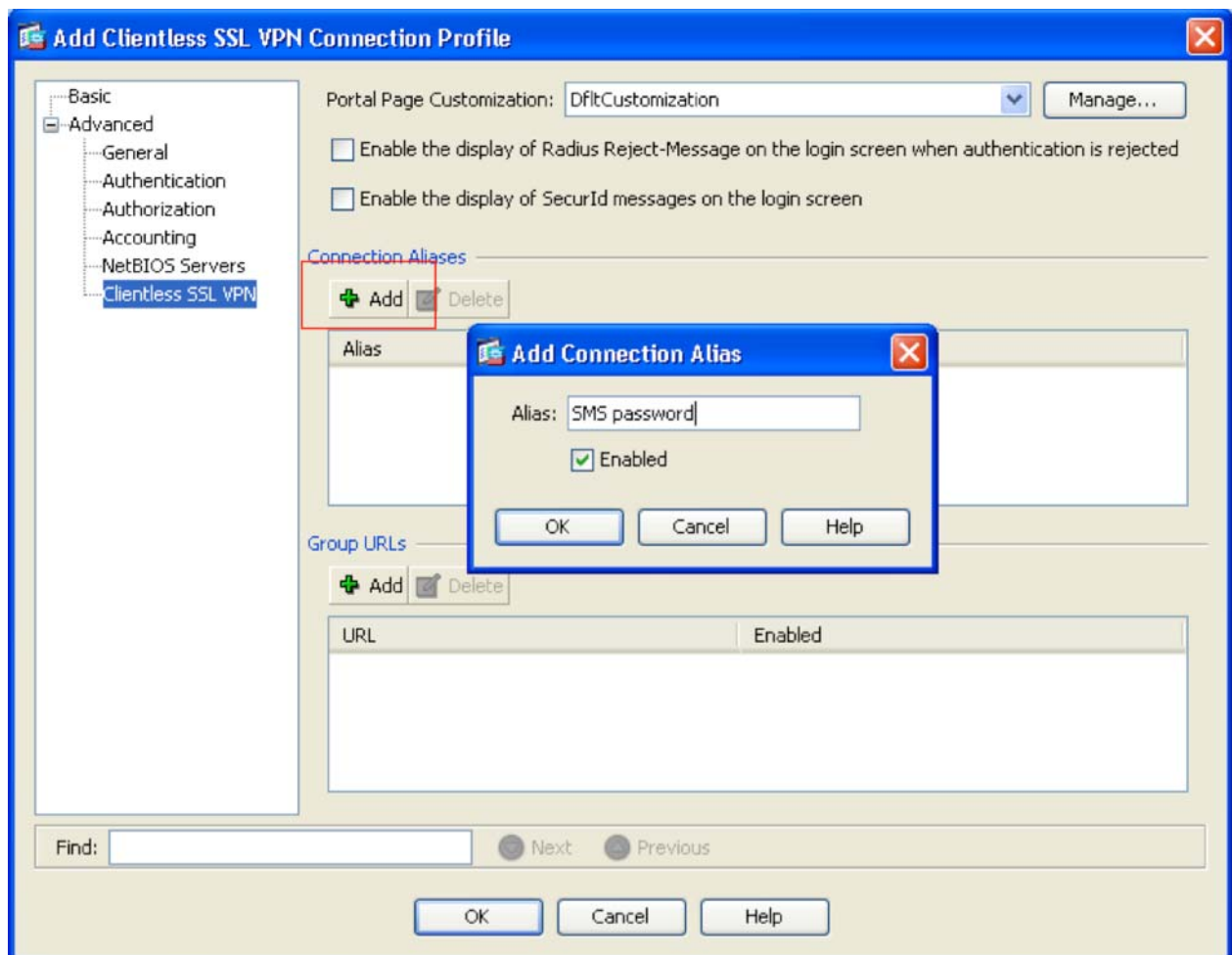
## 9.6.3 Specify AAA Server Group = OTPserver





## 9.6.4 Edit Connection Profile Clientless SSL VPN Settings

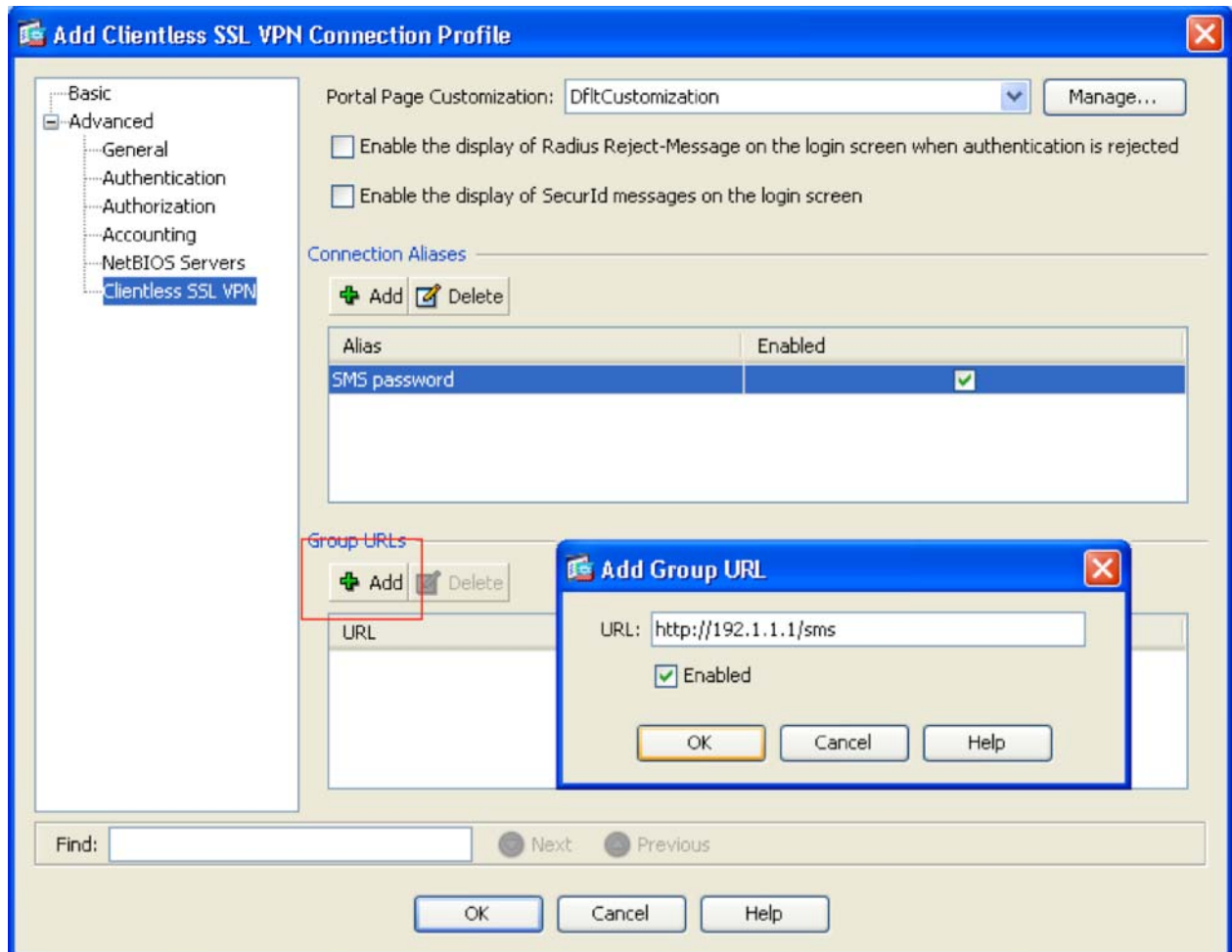
## 9.6.5 Add Alias if user should be able to select authentication method by drop-down-list





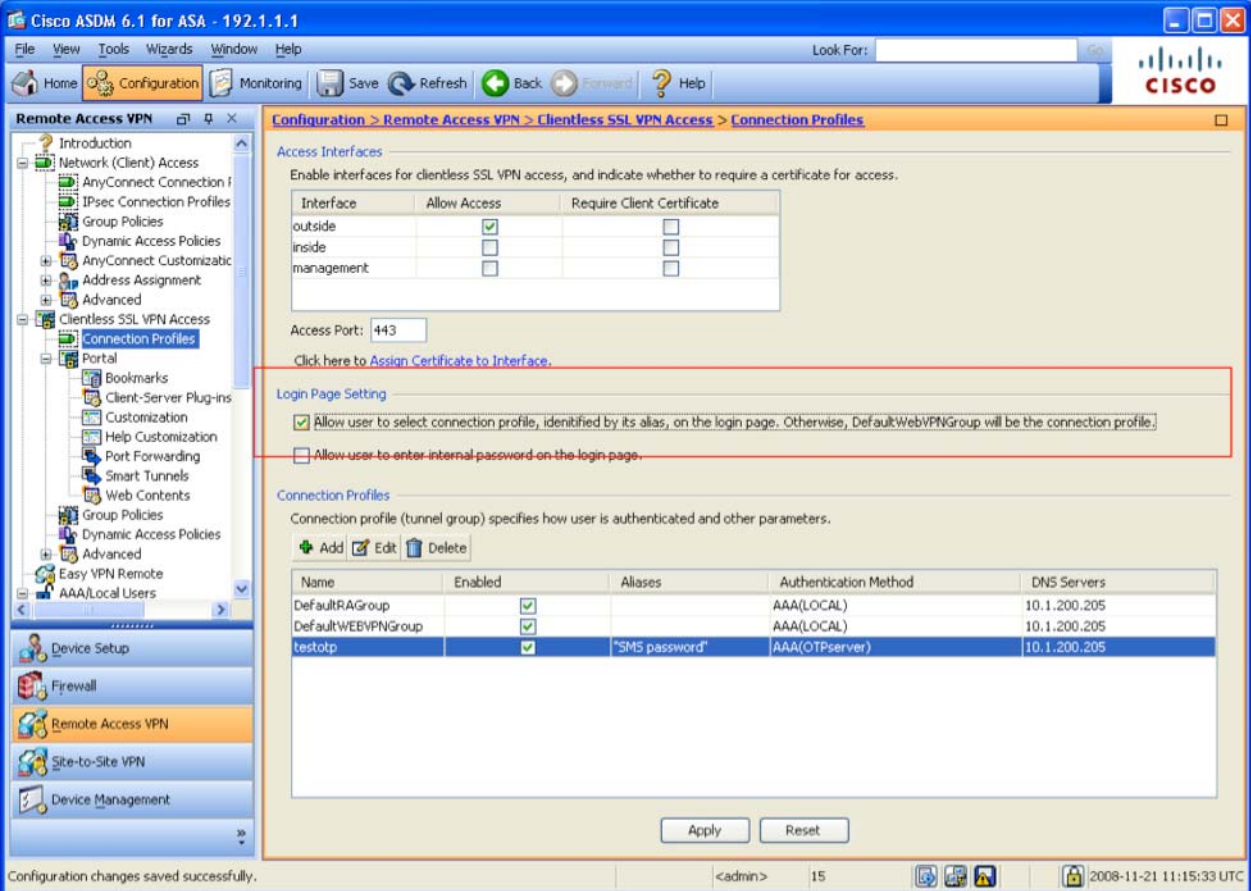
### 9.6.6 Edit Connection Profile Clientless SSL VPN Settings

### 9.6.7 Add Group URL if user should be able to select authentication by specifying URL



### 9.6.8 If user should be allowed to select authentication method by drop-down-list,

### 9.6.9 select this item.



The screenshot shows the Cisco ASDM 6.1 for ASA - 192.1.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles' page.

**Access Interfaces**

Enable interfaces for clientless SSL VPN access, and indicate whether to require a certificate for access.

Interface	Allow Access	Require Client Certificate
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>
management	<input type="checkbox"/>	<input type="checkbox"/>

Access Port: 443

[Click here to Assign Certificate to Interface.](#)

**Login Page Setting**

☒ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☐ Allow user to enter internal password on the login page.

**Connection Profiles**

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

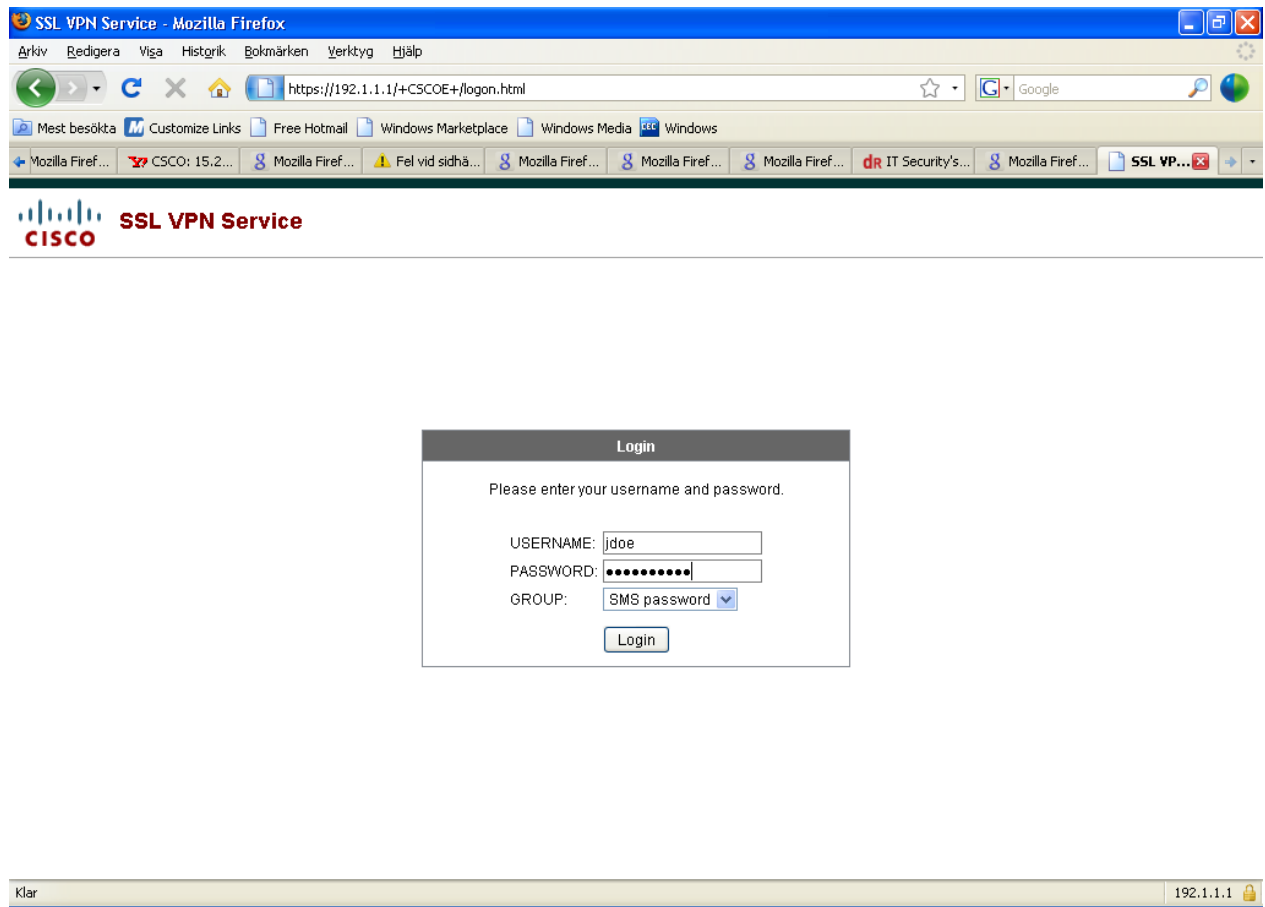
[Add](#) [Edit](#) [Delete](#)

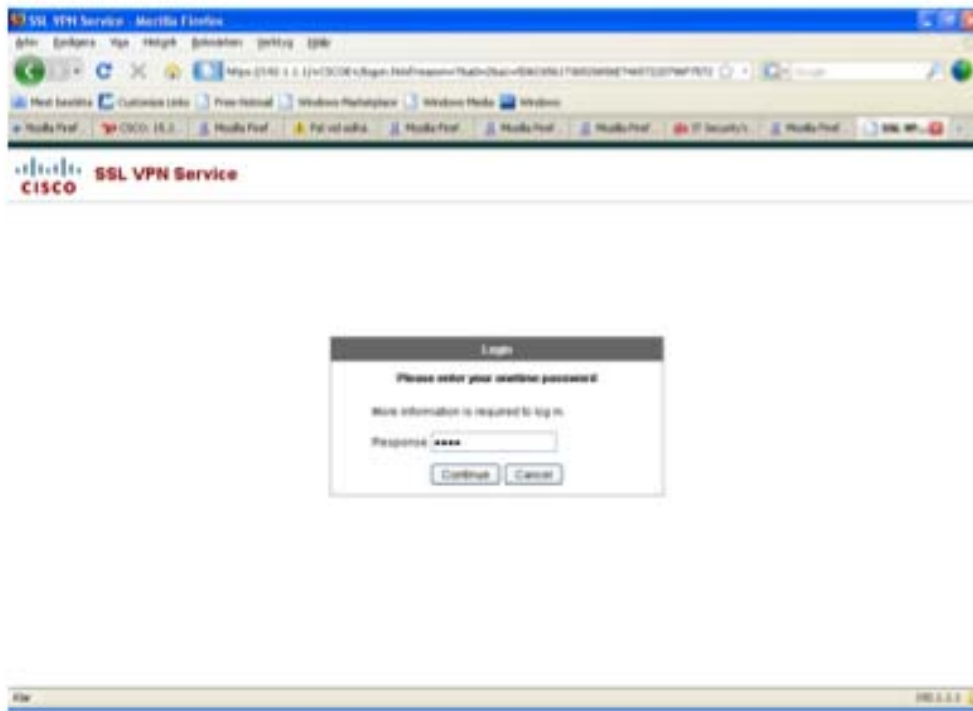
Name	Enabled	Aliases	Authentication Method	DNS Servers
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	10.1.200.205
DefaultWEBVPGGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	10.1.200.205
testotp	<input checked="" type="checkbox"/>	"SMS password"	AAA(OTPserver)	10.1.200.205

[Apply](#) [Reset](#)

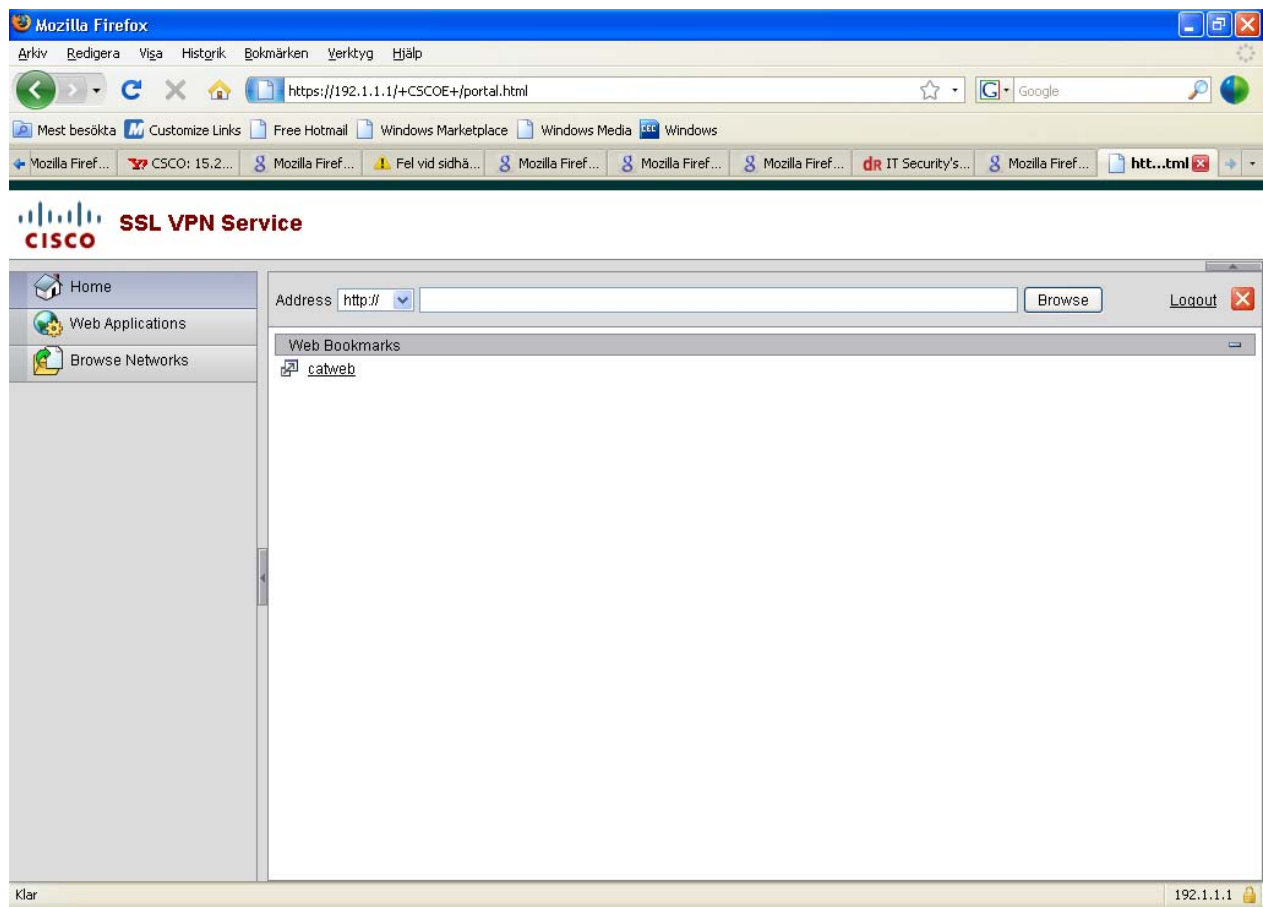
Configuration changes saved successfully.

<admin> 15 2008-11-21 11:15:33 UTC



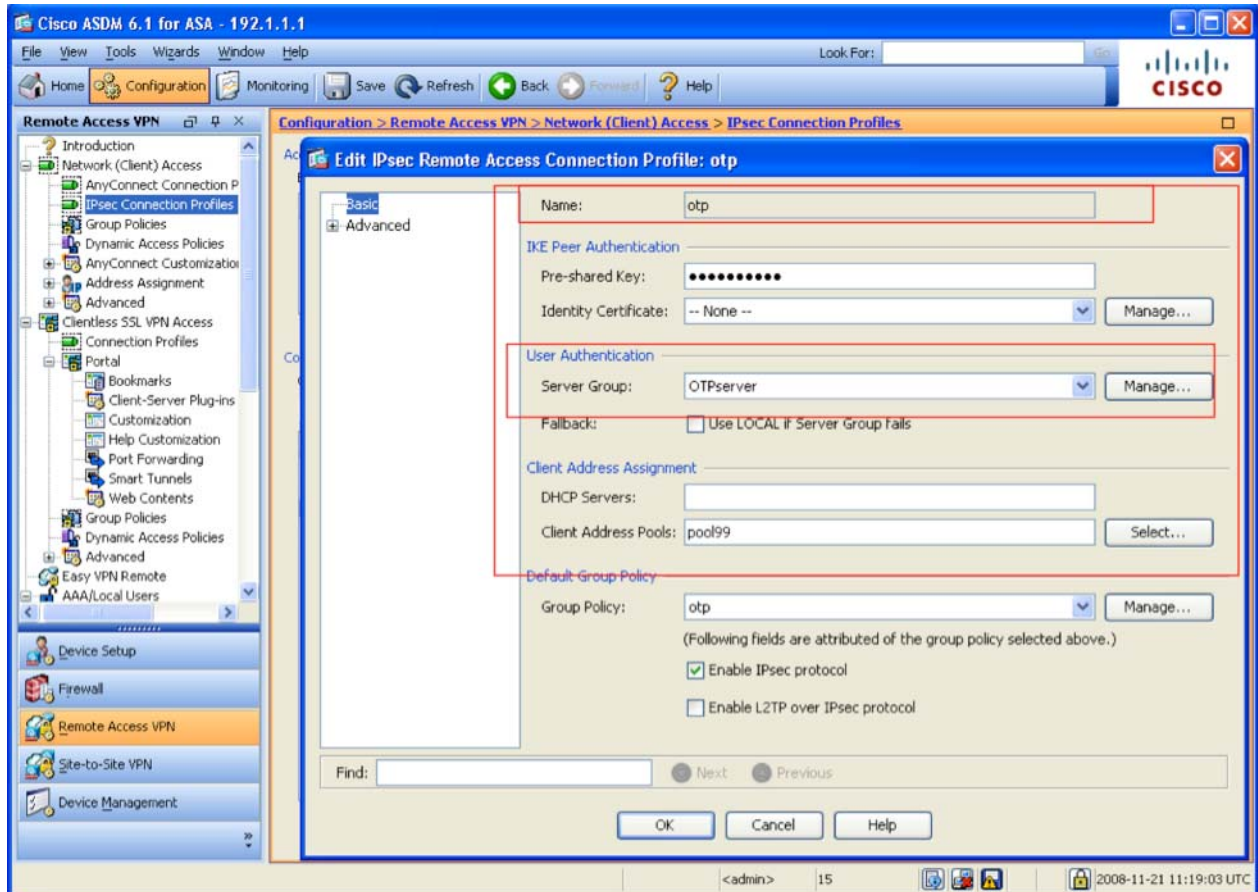


**Login successful, the user will now get to his portal, which can be customized depending on Active Directory membership, PC health status ( antivirus , hotfix etc ) and authentication method**



## 10 Configuring ASA5500 for Cisco VPN Client authentication with Nordic Edge OTP Server

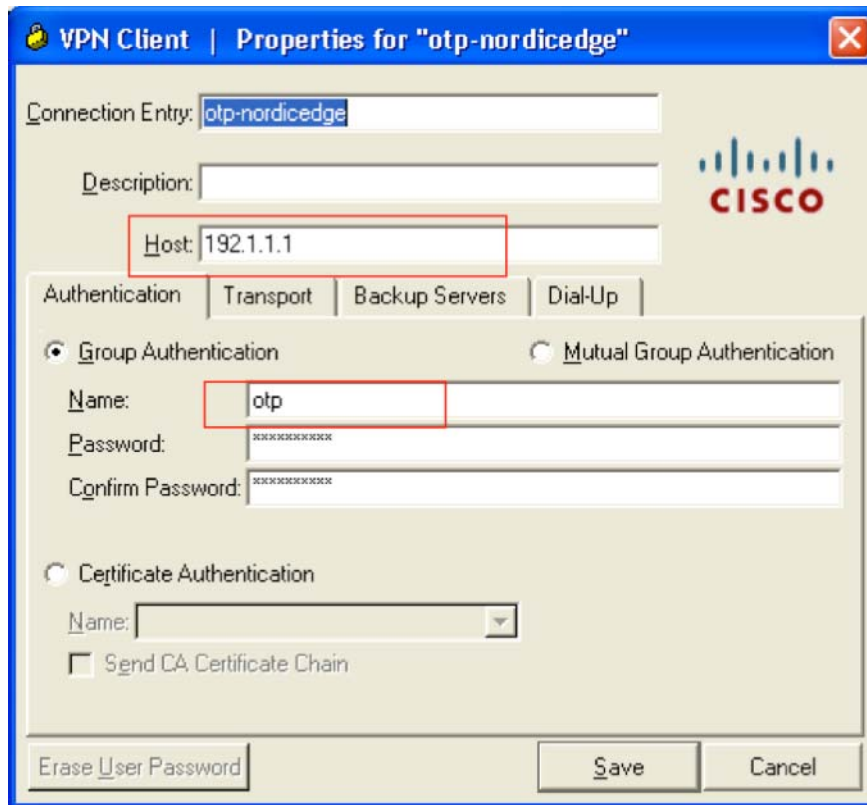
### 10.1 Add a new ( or Edit an existing) Cisco VPN Client Connection Profile to use the OTPserver



## 10.2 At the Cisco VPN Client, create an entry with correct name and password

- Name must match the connection profile name at previous slide.
- Password must match the pre-shared key in ASA5500.

(Note : This can be distributed via MSI installation)



## 11 Start testing

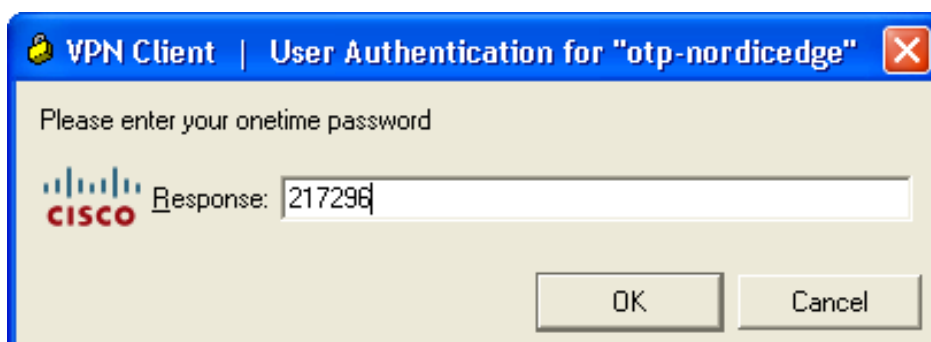
### 11.1 Enter your Userid and password as usual



### 11.2 You will receive a one-time password to your mobile phone within a couple of seconds.



11.3 Enter your one time password and click on “OK”.







## 12 Purchase

If you want to purchase the product, you are more than welcome to contact us at [sales@nordicedge.se](mailto:sales@nordicedge.se) and we will send you an offer. Please note that the price will depend on number of users.

## 13 Technical questions

If you have any technical questions, please contact us at [support@nordicedge.se](mailto:support@nordicedge.se) ---

Thank you for showing interest in our product

The Nordic Edge One Time Password Server Team